Wireless Security and Measures Manual:

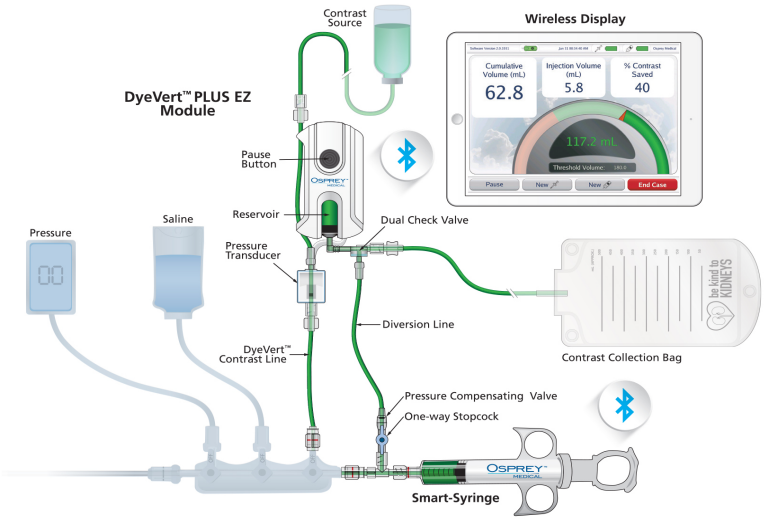
for Bluetooth and Wi-Fi connections of the Osprey Medical Smart Monitor

Contents

Device Description

The device consists of a Smart Monitor, Model Number: “SMART” (Re-order number SMART-XX) to be used with the DyeVert™ Plus Disposable Kit, DyeVert™ Plus EZ Disposable Kit or the DyeTect™ Contrast Monitoring Disposable Kit during controlled infusion for procedures requiring injection of contrast. The Smart Monitor allows for monitoring and display of contrast volumes manually injected.

Smart Monitor



Intended Use/Indications for Use

INTENDED USE

The device consists of a Smart Monitor to be used with the DyeVert Plus Disposable Kit, DyeVert Plus EZ Disposable Kit or the DyeTect Contrast Monitoring Disposable Kit during controlled infusion for procedures requiring injection of contrast media. The Smart Monitor allows for real-time monitoring and display of contrast volumes manually injected.

INDICATION FOR USE

The device consists of a Smart Monitor to be used with the DyeVert Plus Disposable Kit, DyeVert Plus EZ Disposable Kit or the DyeTect Contrast Monitoring Disposable Kit during angiographic or CT procedures requiring controlled infusion of radiopaque contrast media.

Smart Monitor Hardware and Software Overview

The Smart Monitor utilizes an Apple iPad Mini. A 10 foot (3m) lightening power cord is securely attached to the Smart Monitor Clamp. The Smart Monitor Clamp is adhered to the back of the Smart Monitor. Electrical requirements are 100-240V, 0.5A (0,5A), 50-60 Hz.

Smart Monitor, Model Number: SMART-US is to be used with the DyeVert™ Plus Disposable Kit, DyeVert™ Plus EZ Disposable Kit or the DyeTect™ Contrast Monitoring Disposable Kit during controlled infusion for procedures requiring injection of contrast. The Smart Monitor allows for monitoring and display of contrast volumes manually injected.

The Osprey application runs on the Smart Monitor that utilizes an Apple iPad Mini. The Apple iPad Mini runs iPadOS, an industry-leading operating system with security and data protection designed into the system at every layer including the custom processor, OS design, process isolation, and detailed review per application. Apple maintains a readable security document for iPadOS at https://www.apple.com/ that contains many more details about security and privacy on iPadOS devices like the Smart Monitor with iPad Mini.

All iPads are purchased, registered, and deployed with Apple's Device Enrollment Program (DEP). DEP provides Osprey with the ability to configure iPads using Apple's Mobile Device Management (MDM) program. MDM is an Apple-approved method of provisioning, monitoring, and securing iPadOS devices.

If the Smart Monitor is connected to the internet via Wi-Fi, the iPad Mini communicates with an MDM server. Osprey uses the MDM server to configure the Smart Monitor and "lock down" the Smart Monitor to mitigate a variety of risks, to monitor activity on the Smart Monitor, and to keep the Smart Monitor up-to-date with OS and Osprey application updates. All MDM data are encrypted in transit and at rest. All interaction with the MDM is logged via an audit trail. Audit logs include user, date, time, activity and Smart Monitor serial number. To obtain a copy of the audit logs, please contact Osprey Medical.

During a case, the Smart Monitor collects and stores a variety of data, including the case start time and date, information about the contrast saved and used, and the raw data received over Bluetooth Low Energy from the disposable devices. All data on the Smart Monitor is encrypted at rest with AES-256. More details about iPadOS security are available at https://www.apple.com/.

If the Smart Monitor is connected to the internet via Wi-Fi, the Smart Monitor uploads this case data to Osprey nightly. The files are uploaded to Amazon Web Services (AWS) Simple Storage Service (S3) into a unique location for each Smart Monitor. Each Osprey application is assigned credentials which authorize access to specific S3 buckets. The security policy only allows uploading of data, and the

Osprey application cannot read any files stored in S3, including its own uploads. Access to S3 requires two factor authentication with a dongle being one factor. All access to S3 is logged. More details about AWS S3 security can be found at https://aws.amazon.com/security/.

Wireless Quality of Service

The Smart Monitor utilizes Wi-Fi of an iPad mini to communicate with mobile device management (MDM) and amazon web services (AWS). These communications are not critical to the procedure as this device is not required to be connected to Wi-Fi before, during or after a case. The Smart Monitor is for real-time monitoring and display of contrast volumes manually injected which does not require a Wi-Fi connection. The Smart Monitor has memory to store all data in onboard non-volatile memory. Thus, if a period where the Smart Monitor is unable to communicate with AWS occurs, the device will store this data and communicate it to AWS as soon as a connection can be established. With respect to the loss of data due to limited quality of service, the system provides for confirmation logs that all data have been communicated from the Smart Monitor to AWS.

Antivirus

There is no supplemental antivirus protection needed for iPadOS devices. Please see https://www.apple.com/ for more details.

Smart Monitor Configuration

The MDM setup configuration allows for configuring the iPadOS device's WiFi settings, setting and locking the wallpaper, hiding iPadOS apps in the launcher except for Settings and desired apps, and preventing the user from receiving iPadOS notifications. Other MDM capabilities include locking, locating and wiping iPadOS devices, locking an arbitrary app into "Kiosk" mode so that the user cannot leave the Osprey application until the end of a case, and preventing iPads from being accessed via a lightning cable.

After applying the setup configuration, the Smart Monitor users will only be able to access the following features:

- DyeVert Plus app
- eGFR Calculator app (National Kidney Foundation)
- Settings app (with restrictions via MDM)

MDM is also used to lock down various iPadOS features and settings. For example, the Osprey Smart Monitor (DEP iPad Mini's) are specially configured to only make certain apps available to the user and sets restrictions on what the user can change in settings. Multiple other security features are also in

place to prevent unauthorized access to Osprey app data including preventing iPad Mini's from being accessed via a lightning cable. See Attachment A – MDM Security Features for more details.

System Updates

Osprey tests OS updates before they are released to the public in order to determine if any compatibility updates are required for the Osprey application. These application updates will be automatically updated via MDM on Smart Monitor that are connected to Wi-Fi. The MDM commands can also be used to specifically target devices for OS and app updates.

Password Control

When using the device there are no individual logins, instead a shared passcode is used. MDM requires a passcode to be set on the iPad. This passcode enables iPadOS's default storage encryption (AES-128), which protects data at rest on the iPad. If the end user changes the password, that information will not be available to Osprey Medical. If the iPad is suspected to be compromised or a changed password is unknown, the passcode can be reset remotely at any time via MDM.

The only data that the device is capable of showing to the user is "case history", which shows the date of the case and start time, cumulative contrast used, cumulative contrast saved, percent contrast saved, and percent of contrast threshold injected for recent cases.

Encrypted Data Storage & Transfer

Smart Monitor

MDM requires a passcode to be set on the iPad Mini. This passcode enables iPadOS's default storage encryption, which protects data at rest on the iPad with at minimum AES-128. Additionally, all MDM data and commands are encrypted at rest (AES-256) and in transit using TLS (Transport Layer Security).

AWS

All data transferred via the AWS library requires secured connections using Transport Layer Security (TLS) certificates. The data is encrypted in transit, as all connections made to AWS use endpoints that support encrypted transit with HTTPS.

The app provides secure data export (encrypted and authenticated). Uploaded data is encrypted (AES-256) at rest on AWS and is secured in transit using TLS (Transport Layer Security) when being accessed.

Access Control

Smart Monitor

Apple's MDM protocol is leveraged to ensure only trusted content is accessible by the user. The Osprey app is only available on Osprey Smart Monitor (DEP iPad Mini's) and cannot be found on Apple's App Store. This helps prevent unauthorized use by limiting access to specific devices.

MDM

The MDM platform can only be accessed with secure credentials, requiring all Osprey Medical authorized personnel are authenticated & authorized to send MDM commands to the Osprey DEP iPads.

Administrator access to the MDM system requires an individual account with a password of 8 characters or longer. When any MDM system changes occur, they are logged and can be viewed by an administrator.

AWS

Each iPad is setup with write-only access keys to push case data to Osprey's private & secured Amazon Web Services (AWS) S3 bucket. This way, the access keys cannot be used to access or read any other Smart Monitor data.

Uploading data via WiFi requires non-hardcoded individual credentials per iPadOS device, configured via MDM. The credentials assigned to the Smart Monitor are not capable of reading their own files or other Smart Monitor accounts' files. Access to data on AWS requires individual credentials and updating the configuration requires two-factor authentication.

All AWS credentials are setup with role-based (read-only, write-only, administrator) permissions to limit access.

Activity Audits

All hospital user activities are logged on the Smart Monitor and all Osprey personnel activities are logged in AWS and MDM allowing for audits and tracking. Any actions can be identified by the Smart Monitor's iPad Mini serial number and all AWS or MDM actions are logged with the account information

to tie back to a specific Osprey user. This includes the ability to generate reports that identify which Osprey user accessed what features at what time.

AWS

All activity for uploads and data modification on AWS are logged. User and administrator activities are logged in AWS's CloudTrail service. S3 buckets are setup with server access logging enabled to record details about access requests. Server access logs are stored in S3.

Administrator access including the modification of these rules or groups in AWS is logged and access is restricted to the minimum number of individuals. Additionally, any administrator modification of ePHI is logged in CloudTrail and the ePHI bucket's server access logs.

Smart Monitor

The MDM can generate reports showing the last time each device connected to the MDM system that include; the installed version of iPadOS and application(s) on each device, the available storage space on the iPadOS device, and any jailbroken devices.

PHI Data Security

Data is enter-only in the Osprey app on the Smart Monitor. Users of the application cannot view or access Patient ID or eGFR data once it's been entered. The data is stored in a separate Clinicals Database on the Smart Monitor. It cannot be modified once it's written to the Clinical Database.

All Osprey app data including ePHI data is in encrypted (AES-128) storage on the iPad. All data stored by the Osprey app on the Smart Monitor is not available via iTunes File Sharing due to MDM policies and is not available via other applications due to inherent iPadOS sandboxing. The Clinical Database containing PHI data is pushed to a different AWS S3 cloud storage bucket than the rest of the case data. By default this capability is disabled on the Smart Monitor. Only facilities that have a specific agreement with Osprey Medical for collection of ePHI data will be provided with Smart Monitors configured for ePHI data collection in AWS S3. Smart Monitors that are not configured for ePHI data collection will NOT upload data to the AWS S3 ePHI data cloud storage bucket even if the data is entered on the Smart Monitor.

If a Smart Monitor is suspected to be compromised, it can be wiped remotely using MDM commands so that all data are deleted. If the Smart Monitor is not connected to a Wi-Fi network, the ePHI data will be inaccessible since the Osprey application data is under protected storage and cannot be accessed by the application or any user.

For uploads, the Smart Monitor only has write-only access to AWS. This ensures that the Smart Monitor cannot access, read or modify any ePHI data in cloud storage, as the iPad access keys are only allowed to write data. The credentials for AWS access can be remotely modified and removed if needed via MDM. Since PHI data can't be accessed or modified once input on the Smart Monitor there is no way for data to be corrupted before being pushed to AWS.

Once uploaded to AWS, the PHI data is again under encrypted storage (AES-256). AWS S3 is one of the most reliable cloud storage options with minimal downtime. Additionally, AWS supports HIPAA-compliant services and high security configurations. For instance, two-factor authentication is required to log in and access ePHI data. Only Osprey personnel authorized to view PHI data are given credentials to access the PHI data. The AWS credentials can be customized per user to limit access to unnecessary ePHI data.

All AWS services used are HIPAA-eligible and are designed to support the administrative, technical, and physical safeguards for HIPAA compliance. Once on AWS, the data cannot be modified since authorized Osprey personnel with PHI access only have 'read-only' access and thus are able to read data but prohibited from writing or deleting any data. This reduces the likelihood of PHI data being improperly altered or destroyed.

For more information regarding AWS's HIPAA compliance, see:
https://aws.amazon.com/compliance/hipaa-compliance/

Security Administration

Per Osprey Medical internal procedures, security checks are performed on a regular basis. These checks include reviewing ISAO notices as well as reviewing new versions of iPadOS, MDM, AWS, and other Software of Unknown Provenance dependencies for security patches. All MDM and AWS users and groups are reviewed to ensure the correct permissions are applied and access is restricted to the minimum number of individuals.

New iPadOS versions are reviewed as they become available through Apple Developer's Beta SW Program. New MDM server versions are reviewed as they are announced.

Osprey employees perform security awareness and training before interacting with any of the systems mentioned in this document.

Vulnerability Management

MedISAO vulnerabilities and cybersecurity notices are reviewed each month in order to ensure the system is not affected by newly reported threats. If a vulnerability impacts the Osprey Medical Device system, risk management deliverables will be updated and when possible a new software update or patch will be released to fix or reduce vulnerability.

If a vulnerability is discovered or reported for the Osprey Medical Device system, it will be reviewed, disclosed, and submitted to MedISAO.

Disaster Recovery

In the event of a cybersecurity breach, the Osprey system is able to detect, respond and recover. All activities on MDM are logged as well as all events that occur in the Osprey app. These logs provide Osprey with the ability to trace and diagnose issues. MDM can be used to remotely wipe devices in the case that an iPad becomes a security threat. MDM also supports the ability to push out iPadOS and Osprey app updates to provide users with the latest cybersecurity patches.

If any MDM or AWS users are identified as compromising security, administrators can remove access privileges.

Appendix: MDM Setup Configuration

The MDM setup configuration allows for configuring the iPadOS device's WiFi settings, setting and locking the wallpaper, hiding apps in the launcher except for Settings and Osprey enabled apps, and preventing the user from receiving iPadOS notifications. Other MDM capabilities include locking, locating and wiping iPadOS devices, locking an arbitrary app into "Kiosk" mode in which the home button does not open the launcher screen during a case, and preventing iPads from being accessed via a lightning cable.

After applying the setup configuration, the Smart Monitor users will only be able to access the following features on the iPad Mini:

- Osprey DyeVert Plus app
- eGFR Calculator app (National Kidney Foundation)
- Settings app (with restrictions via MDM)

After applying the setup configuration, the Smart Monitor users will not be able to access or use the following features on the iPad Mini:

- iCloud login via Apple ID
- AirPrint printing
- Airplay screen mirroring
- App Store
- Camera
- Airdrop
- iMessage
- Voice dialing
- Siri
- Siri suggestions
- Apple configurator profiles
- iTunes / iTunes store
- Removing system apps
- Apple music
- Radio
- Erase all contents and settings
- Accept untrusted TLS certificates

- Automatic updates to certificate trust settings
- Trusting new enterprise apps
- Installing configuration profiles
- Add VPN configurations
- Classroom App
- Account settings
- Bluetooth settings
- Find my Friends
- Modify notification settings
- Modifying restrictions
- Modifying wallpaper
- Pairing with computers via lightning cable
- Documents sharing
- Handoff
- Sending diagnostic data to Apple
- Touch ID/Face ID
- Pairing with Apple Watch
- Predictive keyboard
- Keyboard shortcuts
- Auto correction
- Spell checking
- Define word
- Dictation
- Wallet app
- Notification Center in lock screen
- Today view in lock screen

The MDM App Configuration allows certain configuration settings to be passed to the Osprey DyeVert Plus app. These configurations must be set for each individual Smart Monitor.

These settings are passed to the Osprey DyeVert Plus app through MDM:

- AWS S3 User Name
- AWS S3 Access Key
- AWS S3 Secret Key
- AWS S3 Bucket
- AWS S3 Upload Path
- AWS S3 Clinicals Bucket (default is disabled)
- AWS S3 Region
- Osprey Settings Passcode
- iPad Serial Number
- Injection Event Dwell Time
- Case Auto End Time
- Screen Recording Enable/Disable (default is disabled)

Australian Sponsor
Osprey Medical, Pty
Level 13, 41 Exhibition Street
Melbourne, Victoria 3000 Australia

EC REP

MedPass SAS
95 bis Boulevard Pereire
75017 Paris - France

℞ only CE 2797

Refer to Instructions for Use for Contraindications, warnings, precautions and directions for use.

Osprey Medical
5600 Rowland Road, Suite 250
Minnetonka, MN 55343

www.ospreymed.com
Phone: 952.955.8230
Fax: 952.955.8171

customerservice.ospreymed.com

Customer Service Toll-Free
Phone: 855.860.7584
Fax: 855.883.4365