Security Specs

How Flex VRA® protects your network and your patients' privacy.

Flex VRA® **needs no network**, has **no cameras or microphones**, takes commands only from its own **paired 433 MHz remote** and **stores no patient information**.

Specifications

Network connection	None required; ships with none set up
Inbound connections	Blocked by a Windows Firewall rule; no open ports
Wireless control	433 MHz radio (no Bluetooth or Wi-Fi)
Remote pairing	Each remote paired to its own reinforcers only
Cameras and microphones	None built in
Patient information	None entered, stored or transmitted
Screen Mirror stills	Permanently deleted when Screen Mirror closes
Kiosk Lockdown	On by default; no route to the Windows desktop
Service PIN	Optional, 4–8 digits; stored as a salted one-way hash
PIN lockout	30 seconds after 5 wrong tries
Security audit log	Kept 2 years; no patient information
Software updates	Offline, by USB; SHA-256 integrity check
Remote support	Attended, on request only; no remote-access agent
Stored passwords or secrets	None
Operating system	Windows 10; Windows 11 available on request

Why it matters

Built to work without a network

Flex VRA® opens no network ports and ships with no Wi-Fi or Ethernet connection set up. It cannot be scanned or reached from outside the building, and it doesn't become a way into your hospital network.

No cameras or microphones

Flex VRA®, Flex Toy and Flex Halo reinforcers only show light, video and sound, so they cannot see or hear the booth. The optional Flex Cam connects to the clinic's own computer, not the reinforcer.

A paired radio, not Bluetooth or Wi-Fi

Commands travel over a 433 MHz link from the Flex remote or the Flex PC USB transmitter. Each remote is paired to its own reinforcers and cannot control any other device, and nothing shows up in a phone's Bluetooth or Wi-Fi list.

A locked-down device

Kiosk Lockdown, on by default, hides every route from Flex VRA® to the Windows desktop. Clinics can also require a service PIN, stored only as a salted one-way hash.

A security audit log

Service menu access, PIN tries, Lockdown changes, updates and shutdowns are recorded in their own log for two years. Staff can save it to a USB stick for a security review.

Offline, integrity-checked updates

Updates and new content arrive on a USB stick from Flex VRA® and are installed by clinic staff. Nothing is downloaded over the internet, and every file is checked against its SHA-256 fingerprint.

Questions from hospital IT

Does Flex VRA® connect to the internet or our network? No. It needs neither and ships with no network set up. It opens no ports, and a Windows Firewall rule blocks all inbound connections to it.

Does it store or transmit patient information? No. There is nowhere to enter patient details and no database. Logs record what the system did, never who was tested.

Can it be accessed remotely? Only for attended support. If a clinic asks for help, it connects the monitor and a technician starts a session with them. There is nothing listening in the background.

How do we report a security concern or request an MDS2? Email sales@flexvra.com. We will confirm we received your report and keep you updated.

Learn more at flexvra.com/security. Specifications describe Flex VRA software as shipped and may change. Flex VRA® is a registered trademark of Flex VRA, LLC.