integrity™ V500

vivosonic

Cybersecurity Information and Risk Transfer To Customer

This Integrity System was shipped with the most current version of Integrity software version effective on the date of shipping.

a. The Integrity™ V500 System has gone through rigorous verification and validation by Vivosonic (the manufacturer) for the current software version on the model of the Windows Computer that currently ships including all Windows updates as at the release date for both Windows 10 and Windows 11.
b. Cybersecurity Vulnerability Scans were performed on the current Integrity software version in both Windows 10 and Windows 11 as at the release and no vulnerabilities were detected.
c. The Company monitors the Cybersecurity status of the current release of Software on a regular basis and posts the updated status at Vivosonic.com/customer-support/cybersecurity

Background

The Integrity V500 System is a Windows Laptop PC based standalone diagnostic device that **does not require any networking ability to function.**

The Device includes the Windows Laptop PC,the Clinician PC. This Clinician PC interface communicates via Bluetooth/Wireless to a portable battery operated Patient Interface module, the Vivolink. This transmission does not include Personal Health Information (PHI). The Vivolink provides auditory stimuli to the patient and connects to the patient with electrodes to measure recorded responses. Data collected on the Vivolink is sent via Bluetooth/Wireless back to the Clinician PC for processing, analysis and Clinician review. Test results are stored on the local hard drive of the Clinician PC in the Integrity Application Database.

Cybersecurity and Software Responsibilities Transferred to the Customer

The customer understands that the Integrity V500 System as provided can be used as a standalone device with no connection to the Internet. The Integrity V500 System is configured with the main user having Administrative Rights.

The Customer understands the following:

1. Customers (Clinicians) determine the extent of Patient Health information stored on the device.
2. Vivosonic does not have access to the Integrity system at the Customer premises without the permission of the Customer to allow remote access via VPN.
3. Windows Defender is activated on the Integrity Laptop.
4. Autoplay on the USB Ports has been disabled and scanning of USB media is enabled with Windows Defender.
5. For Integrity 9 series software versions, Personal Health Information in the Integrity Database Records are encrypted and are only visible from withing the Integrity Application.

6. The Integrity System can be configured so that when the Integrity Application is exited there is a backup of the database saved as an additional file
7. Application Users and Logins can be set up if required by the Customer. Activities are logged relative to the User.
8. For Integrity 8 series software versions, all Integrity Users require Administrative rights for running the Integrity Application.
9. For Integrity 9 series software versions, Administrative rights are only needed to update the software. Integrity Application users(Clinicians), do not need Administrative rights for running the Integrity Application.
10. Vivosonic will post on Vivosonic.com/customer-support/cybersecurity the most recent Windows Operating system where the Integrity Application functionality has been confirmed and the profile date of the most recent vulnerability scans.
11. Vivosonic will update its Integrity system software image at least every 3 months or when there is a software change associated with Integrity functionality or new Cybersecurity Vulnerability.

The Customer understands and accepts the responsibility:

1. For maintaining backup copies of the database from the Integrity Application on a separate storage device and for managing the cybersecurity risk of that device.
2. For ensuring that database records are not improperly edited or deleted.
3. For establishing Integrity Application Users and Logins for the Clinicians, if required, and ensuring the Users have the applicable administrative rights depending on the Integrity Software series (8 or 9).
4. For managing connections to their network or the internet if required.
5. For performing Window Operating system updates and associated Windows hardware driver updates on a timely basis and also for performing Windows Security updates on a timely basis after reviewing the status of Vivosonic software and windows updates on the Vivosonic website. Vivosonic will post on Vivosonic.com/customer-support/cybersecurity if a Windows Operating system update negatively affects the Integrity Application operation or if Integrity functionality has been verified with the update. An update from Windows 10 to Windows 11 should be discussed with Vivosonic Support as it may require an Integrity software update.
6. The Customer may choose to use an alternate Antivirus software or may load other application software including printers on the Integrity PC. The customer is responsible for ensuring that these applications do not affect the clinical operation of the Integrity Application. The Customer is responsible for maintaining the updates on this additional software and for monitoring cybersecurity risks and scans associated with this additional software.
7. For providing and limiting Vivosonic remote access to the Customer Integrity system via VPN.
8. For preventing the transfer of PHI to Vivosonic when providing Computer for repair or when providing test record or printouts of test records.