8. Pod Cyber Security Guidelines

Device Interface

• The Pod device cannot interface with other devices using connectors, physical means, or Bluetooth or Wi-Fi.
• The device interfaces with the Capsule via short range RF antenna.
• The device interfaces with Vibrant Cloud via a secured encrypted cellular connection.

Cyber Security Protected Design

The device and Cloud system are designed to provide several features that protects the system against cyber threads:
• Device firmware is encrypted to prevent any changes in firmware by uncertified personnel.
• The device does not store any patient sensitive data.
• The communication between the components (device and cloud) is encrypted.
• Device firmware can always be restored from the cloud via a firmware update process.
• The device works on propriety firmware and therefore very hard to access.
• The device is embedded with an Anti-Malware software that can be updated remotely and creates a protected firmware, such that in runtime, the mitigation code detects and block exploitation attempts.
• In case of exploitation attempt detection, the Anti-Malware transmits an alert to the Cloud server using the Pod cellular modem.
• The device firmware is not accessible for the user, therefore no access to any system log files is permitted for the user.

Cloud Connectivity

The device and Vibrant Cloud system are designed to provide several features that protects the system against cyber threads:
• The connection with the Vibrant Cloud system is initiated by the Pod and allowed with a valid security certificate.
• Vibrant Cloud is USA HIPAA legislation certified to provide maximal IT protection means.
• All device logs and data are stored in the cloud system and not locally on the device.
• The device and treatment configuration are kept at the cloud and can be restored.
• The system is ready for use. No system settings are required either for using the treatment or for connecting the Pod with Vibrant Cloud.

Vulnerability Incident Instructions

In case servicing via secure network for servicing is required and in case you've detected cybersecurity vulnerability or incident, you should follow the below instructions:
• If you face difficulties to operate the Pod and use the treatment that could potential be originated by a cyber-attack, please contact Vibrant support. Do not use the device until receiving further instructions.

9. Electromagnetic Compatibility

Table 8: Declaration - Electromagnetic Emissions

Emissions Test	Compliance	Electromagnetic Environment – Guidance
Conducted and radiated RF emissions CISPR 11	Group1 Class B	The Vibrant Capsule System uses RF energy only for its internal function. Therefore, its RF emissions are very low and are not likely to cause any interference in nearby electronic equipment.
Harmonic emissions IEC 61000-3-2	Class A	The Vibrant Capsule System is suitable for use in home healthcare (“home use”) and professional healthcare facility (“hospital use”) environments.
Voltage Fluctuations and Flicker IEC 61000-3-3:2013	Complies	