PHILIPS

Philips Healthcare

# Description of Software Security Requirements for U-NII Devices

## GoSafe Model 7100MHB & GoSafe 2 Model 7150MHB

## FCC ID number BDZ7101MHB
## IC Canada number 655C-7100MHB

**Scope:**
The purpose of this document is to provide a description of the Software Security Requirements for U-NII Devices for the 7100MHB and 715MHB devices. The WiFi 5GHz band operates at 5.15 – 5.25GHZ (U-NII 1) and 5.725 – 5.850GHz (U-NII 3) sub ranges only. The DFS is not part of the scope of this document. Furthermore, the 7100MHB and 7150MHB devices do not have user interface for the WiFi. Therefore, section III of the FCC document "*594280 D02 U-NII Device Security v01r03*" does not apply.

**WiFi Description:**
The WiFi module (WICED WM-AN-BM-23) is used in the 7100MHB and 7150MHB Mobile Help Buttons. The WiFi module is used to establish the user's location. The module supports dual bands 2.4GHz & 5 GHz. The device current configuration excludes the DFS bands.

**Description of Security:**
The following describes the device software/firmware security features:

1. The device WiFi (WICED) module RF parameters (such as transmission power, frequency, data rate, etc.) are preset by the module manufacturer Software Development Kit (SDK). The device application software does not change them, except for the disabling the Dynamic Frequency Selection (DFS) channels.

   The device firmware is validated by the quality assurance team prior to installation. It can only be downloaded or updated at production line with special proprietary application and tool. This application and tool are not available to 3rd party for modification of the device firmware. In addition, the firmware is not available to the public on the company website. The firmware is controlled and protected by the company configuration management system.

Philips Lifeline
111 Lawrence Street
Framingham, MA 01702
USA



PHILIPS Lifeline

2. The application firmware only disables the DFS channels. No other parameters allow the device firmware to control and to exceed the authorized RF characteristics.

3. The firmware is protected by a checksum. If the firmware is modified the checksum will be violated and rejected by production testers.

4. The encryption method used is MD5 HASH.

5. The device in its majority of operation acts as a receiver. The Wi-Fi module is used to scan nearby Wi-Fi access points. The 7100MHB/7150MHB Wi-Fi module only sends active scans (probe requests) to detect nearby APNs every 5 minutes. The active scan transmission time is up to 15 microsecond at a rate between 54-216Mbits/sec with each packet up to 100 bytes (800bits).

   The device firmware does not change the preset RF characteristics in both Client and Active Scan modes. The transmission power has been verified to be with in the permissible limits.

**Conclusion**

The device firmware and WiFi RF parameters are inherently protected against unintentional modifications during manufacturing or intentional unauthorized changes.

Philips Lifeline
111 Lawrence Street
Framingham, MA 01702
USA