SUMMARY OF: P890003/S326 (MASTER), P010015/S255, P010031/S478, P090013/S165, P820003/S132, P850051/S082, P900061/S133, P920015/S146, P930022/S017, P970012/S096, P980016/S514, P980035/S404, P980050/S097, AND P990001/S119

REMOTE CONTROL SOFTWARE FOR THE 2090 PROGRAMMER

Executive Summary

In this 180-Day PMA Supplement, Medtronic is requesting approval for the Remote Control Software (SW036) to be used with the 2090 Programmer. The Remote Control Software is an extension of the FDA-approved RemoteView software (P890003/S249, April 25, 2012). The Remote Control Software will allow a remote operator to control the 2090 Programmer while a local operator monitors the patient. The remote and local operators are expected to maintain a phone connection at all times during a remote session. An Off-the-Shelf (OTS) server application, considered to be software of unknown provenance (SOUP), is used to allow remote access over the Internet. This will be referred to as “OTS server application” throughout this memorandum.

Several concerns arose during the first round of review. The sponsor was sent deficiencies in a letter on March 19, 2015. Interactive discussions occurred after the sponsor received the letter. The sponsor then submitted Amendment 1 to provide formal responses to the deficiencies. Concerns from the first round of review were addressed and FDA recommends approval of this supplement.

Review Team

The review team consisted of a Lead Reviewer (Biomedical Engineer), Human Factors Engineer and Clinician with informal consultation from IEDB members, PMA staff and ODE Digital Health Staff.

Device Description

The Remote Control software is designed to allow authorized remote operators to control the 2090 Programmer. Remote Control sessions are intended to take place in a clinical setting for device follow-up sessions. The local operator is expected to be in the room with the patient and the 2090 Programmer at all times during the Remote Control device follow-up session. Telephone contact between the local operator and remote operator is supposed to be maintained during the entire device follow-up session. See the figure on the next page for a high-level depiction of the Remote Control system.

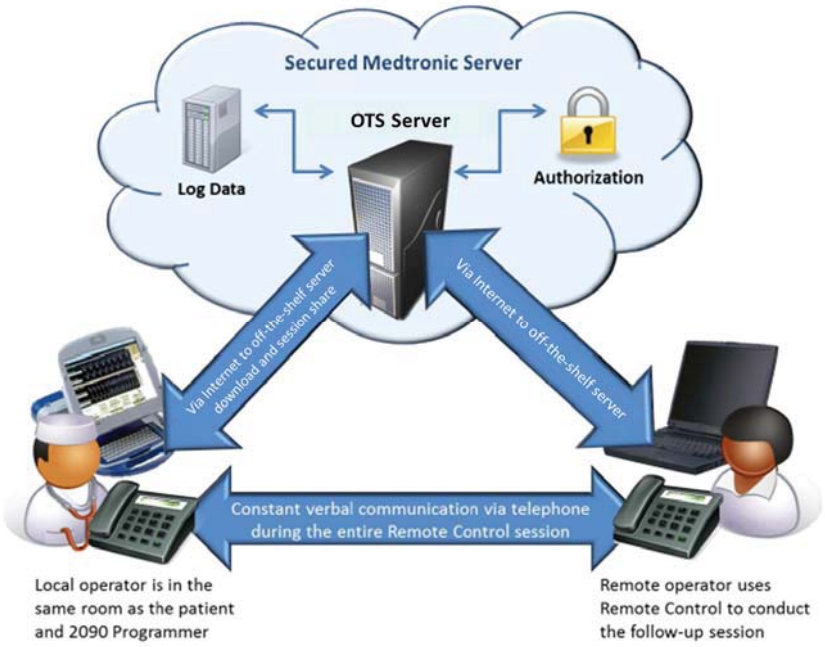


Figure 1: Depiction of Remote Control System

Remote Control software is an extension of RemoteView functionality, approved under Desktop base operating systems software (BOSS) Model 9986, Version 2.6. Remote Control and RemoteView share the same hardware platform, programming language, and data security features.

Remote Control includes use of an OTS server application. The OTS server application provides remote access to the 2090 Programmer by authorized users over the Internet. The OTS server application is already used to allow operation of the previously approved RemoteView software. The OTS server application is considered Software of Unknown Provenance (SOUP) and Medtronic has performed verification and validation specific to this SOUP.

In order to address potential difficulties that may arise when two operators have real time access to the programmer application, Remote Control includes Dual Pen Press and Watchdog features. In the event that the local operator and the remote operator press the screen at the same time, the system will give priority to the pen press of the local operator (Dual Pen Press).The Watchdog feature assesses ongoing connectivity between the Remote Operator and the Local Operator. If the Watchdog detects a loss of connectivity while the pen is pressed on the 2090 Programmer, the Watchdog will issue a “button up” command.

The remote control software has the ability to interrogate and program all devices that can be interrogated and programmed using the 2090 Programmer, including pacemakers, ICDs, CRT-Ps, CRT-Ds and ICMs.

Indications for Use

There is no change to the indications for use for any Medtronic device as a result of this change.

The Medtronic CareLink programmer system is comprised of prescription devices indicated for use in the interrogation and programming of implantable medical devices. Prior to use, refer to the Programmer Reference Guide as well as the appropriate programmer software and implantable device technical manuals for more information related to specific implantable device models. Programming should be attempted only by appropriately trained personnel after careful study of the technical manual for the implantable device and after careful determination of appropriate parameter values based on the patient's condition and pacing system used. The Medtronic CareLink programmer must be used only for programming implantable devices manufactured by Medtronic or Vitatron.

System Users

Remote Control has two users; the local operator and the remote operator. The local operator is present in the room with the patient and the 2090 Programmer at all times during the Remote Control session. The local operator may be a cardiology nurse, technician or other appropriate healthcare provider. The remote operator may be a Device Nurse, Device Technician, Physician or Medtronic Technical Services professional who is an experienced, regular user of the 2090 Programmer who has also received remote control training. Only Medtronic can authorize a remote user and provide credentials for the system.

Remote operators will be trained on the use of the Verbal Protocol as a tool for establishing and maintaining synchronization with the local operators. The Verbal Protocol is spoken by the remote technical support provider (over the phone) to the local operator, who provides verbal confirmation that the protocol is understood.

REVIEW COMMENTS: The issue of this system's users was discussed several times over the course of this review with branch staff members, clinicians, and management. Overall, it was determined that the Verbal Protocol was not sufficient to mitigate the risks of a potentially untrained local operator monitoring the patient and controlling the programmer in emergency situations. Furthermore, it was unclear who would take responsibility for the parameter changes or patient safety in a remote control situation. Deficiencies were sent to the sponsor regarding these concerns.

This topic was discussed heavily during interactive review; the sponsor responded in Amendment 1, stating that the addition of Remote Control functionality does not change the fact that the clinic employee is responsible for the well-being of the patient. The Local Operator is an authorized employee of the clinic who has confirmed prior to initiation of the Remote Control session that he or she is capable of identifying and responding to emergency situations (via the Verbal Protocol). The sponsor proposed a change to the Remote Operator Protocol and the Session Key entry activity, which requires the Local Operator to "tangibly" accept the responsibility to identify and respond to emergency situations (see Principles of Operation section below) and these changes were found to be acceptable by FDA. Furthermore, the sponsor states that it does not make device parameter setting changes without the direction of a physician or nurse who is qualified by license or law to prescribe medical care, including device parameter changes and this will not change with the implementation of the Remote Control functionality. FDA also found this response to be acceptable.

It should be noted that FDA authority over the use of the remote control software is limited to device design, labeling and training. The use of this system will be heavily dependent on practice of medicine, which is not under FDA's jurisdiction. The sponsor specifies qualifications of the on-site programmer user in the labeling and includes instructions on Important Safety Considerations on the local user's tip card. Through interactive discussions, the sponsor clarified that the local user receives "real-time training" via labeling and the verbal protocol to ensure he/she can respond in an emergency situation and check for physical symptoms that are not visible to the remote user. Therefore, FDA has restricted the approval of this device with regards to training as prescribed in the labeling and verbal protocol.

FDA suggested that patient labeling be incorporated into the system (during interactive review) to inform the patient of the potential risks with a remote control session and to confirm that the patient is willing to enter into this scenario. In Amendment 1, the sponsor agreed with FDA's suggestion and proposed that this patient labeling be incorporated into the Verbal Protocol (spoken to the patient via speakerphone) and provided via an eBrochure. FDA reviewed the language proposed and found it to be acceptable. Therefore, this patient labeling will be included in the marketed device labeling.

Language to assign responsibility for parameter changes made during a remote control session was suggested to be added to the remote operator verbal protocol in the March 19, 2015 Major Deficiency Letter. However, the sponsor has provided adequate justification that such language does not need to be included because the physician's responsibility to the patient exists whether it is the physician who personally renders care or if it is another person acting under the direction of that physician. The sponsor described the workflow of the remote control session and ensured that an authorized care provider would be responsible for any parameter changes in such a session. Therefore, FDA agreed that this type of language did not need to be included in the labeling or verbal protocol.

Principles of Operation

The following describes steps to initiate and perform a remote control follow-up session:

1. The first step in using Remote Control is that the Local Operator calls the Remote Operator on the telephone. This call is maintained throughout the Remote Control session.

2. The Remote Operator launches Remote Control on their PC and logs in. At this time, the Remote Operator begins the review of the Verbal Protocol with the Local Operator.

3. The Remote Control server generates a 7-digit Session Key and sends it to the Remote Operator's computer. This 7-digit key is generated only after the remote operator reads and agrees to the following warning (on an external website):

   By clicking "Generate Session Key", I agree NOT to perform the following functions during a Medtronic 2090 Carelink Programmer Remote Session:

   - **Cardioversion**
   - **EP studies/arrhythmia inductions**
   - **Underlying rhythm tests**

4. The Remote Operator provides the Local Operator with the Session Key. This exchange requires the Remote Operator to receive agreement that the Local Operator will remain in the room, next to the patient, at all times during the remote control session, monitor for any signs of distress and report patient status changes.

5. The Local Operator enters Session Key on the 2090 Programmer.

6. The Remote Operator sees the 2090 Programmer Remote Control session in the queue in the Remote Control program and accepts the session.

7. The Remote Operator starts the Remote Control session and can view and control the 2090 Programmer screen on his or her computer.

8. The Local Operator and the Remote Operator continue the Remote Control session. The Remote Operator can operate the 2090 Programmer remotely, but the Local Operator is also able to take control of the 2090 Programmer during the Remote Control session. When they are done with the follow-up session, they will end the Remote Control session.

REVIEW COMMENTS: Originally, in the March 19, 2015 Major Deficiency Letter, FDA suggested that the sponsor lock out functions that were particularly risky if used in a remote control situation (cardioversion, EP studies/arrhythmia inductions, underlying rhythm tests). During interactive review, the sponsor maintained that it was infeasible to lock out these features from over 200 device applications. FDA continued to emphasize that locking out the features was ideal, and again, through interactive review, the sponsor proposed the website advisory as a substitute for this lockout (as described in #3 above). The FDA review team agreed that this was an acceptable approach instead of locking out the risky features. The clinical consultant agreed that the remote operator is clearly advised they are to avoid this inappropriate programming (VF induction for instance).

A new foreseeable risk unique to remote control is the risk that the local user will not be present when an urgent adverse event occurs during a remote session. Programming without a local user present is only possible in a remote programming scenario. Therefore, the sponsor proposed language (in Amendment 1) to be included in the Verbal Protocol (as described in #4 above) stating that the local user should remain by the patient at all times throughout the session and the FDA review team found this to be acceptable.

Software

Level of Concern

The level of concern pertaining to the Remote Control software is a major level of concern. This is because the Remote Control software is used to control the 2090 Programmer applications, which are used to program or interrogate Medtronic implantable medical devices (IPGs, ICDs, CRT-IPGs, CRT-ICDs and ICMs).

Software Requirements Specification

The sponsor provided the software requirements as part of the submission. The requirements align with the design of the system to provide remote users the capability to view and control the 2090 CareLink Programmer from a remote location. The Remote Access System is built upon the existing RemoteView infrastructure and requirements defined for that system. The requirements focus on display, access, connectivity, training, and system effectiveness. The sponsor also provides requirements for connectivity and IT infrastructure. These requirements focus on connection, user authentication, connection logging, session initiation and restrictions on patient health information (PHI) storage.

REVIEW COMMMENTS: FDA reviewed the software requirements during the first round of review and believes they are appropriate for this system.

Architecture and Design

The sponsor provides documentation describing the system architecture, design and interfaces solution. This document explains and illustrates the design and architecture that are implemented.

RemoteView (and therefore Remote Control) is implemented using a commercially available tool (OTS server application). The implementation consists of software on the Programmer, a virtual appliance (software on a server simulating a distinct hardware appliance), and software on the remote computer. Communication occurs through the Internet.

The OTS server application customer client on the Programmer gathers an image of the Programmer display and transmits that image to the remote console (referred to as “screen scraping”). The image is transmitted a “strip” at a time, so when the Programmer screen changes, the image on the console appears to “paint” across the console.

Control of the programmer is enabled for a user on Remote Control (versus RemoteView), and is accomplished by sending the mouse and keyboard events from the remote computer to the programmer.

REVIEW COMMENTS: The system architecture and design description were reviewed during the first round and seemed adequate. Because remote control is a feature of RemoteView that was previously deactivated, the system architecture is essentially the same as the approved software and the addition of the function is documented. It should be noted that this latent functionality was not made clear under the submission for RemoteView. However, FDA does not have concerns with the architecture or design of the system.

Risk Analysis

Risk management activities for this project were performed to identify, analyze, evaluate, and control hazards associated with the Remote Control software.

A failure modes effects analysis (FMEA) approach was used to identify, evaluate, and ensure appropriate risk controls for the risks associated with system failures, including potential patient safety risks. A use-error analysis (UEA) was performed to identify, evaluate, and ensure appropriate risk controls for the risks associated with use-errors, including patient safety risks. For each of the safety risks identified, a hazard analysis was performed to translate the identified failures or use-errors into potential hazards and associated harm outcomes.

According to the sponsor, the potential risks of the Remote Control system were determined to be reduced to as low as possible. Residual risks were evaluated in the context of the foreseeable benefits of Remote Control and the benefits were determined to justify the potential risks associated with the system. The risk management report concluded that the system is acceptable for human use.

REVIEW COMMENTS: FDA believes that the sponsor adequately identified risks associated with the remote control functionality. The risk controls cited are mainly the user interface, verbal protocol, and system labeling to be used by both the local and remote operators. During the first round of review, through discussions with IEDB branch members and management, there was a clear consensus that these risk controls were not adequate. Deficiencies were sent regarding this and were discussed during the interactive review meetings. Changes were made to the language in the labeling and verbal protocol and submitted in Amendment 1. These changes were found to be acceptable and are appropriate risk controls for this software. Please see sections above for more details on changes made to the labeling and verbal protocol.

Traceability Analysis

The sponsor has provided a traceability analysis which links design input requirements to verification methods. For risks associated with the software, each risk is traced to a system risk control (this is described further in the Risk Analysis section above).

REVIEW COMMENTS: The traceability analysis provided was found to be acceptable during the first round of review.

Software Development Environment Description

The main activities related to the development and testing of software on Remote Control included:

- Definition of software requirements
- Definition of software architecture
- Design and Implementation
- Verification and Validation testing

REVIEW COMMENTS: The description of the development environment was found to be acceptable during the first round of review.

Software/System Verification and Validation Studies

Requirements for the software were designed and implemented in groups. When any one group completed System Verification, that group could start System Validation. The groups are defined below:

Group 1: Software component updates and OTS server application upgrade requirements and design

Group 2: IFU (Instructions for Use, i.e. user manual) component updates.

Group 3: Training material creation and post-release reliability requirements.

Software Verification

Integration testing of software units involved bringing new software functionality (including new version of OTS server application) into the overall software system, verifying the proper behavior of the new functionality prior to integration.

REVIEW COMMENTS: I believe the sponsor has adequately assessed the OTS server application as a SOUP product used with the system. The sponsor has incorporated risks associated with the OTS server application into the overall risk mitigation strategy. Furthermore, system requirements that pertain to the OTS server application (should not degrade programmer performance, for example) are incorporated and have been verified. FDA does not have any further concerns with the use of the OTS server application SOUP.

All software requirements have been met and all protocols have passed. There were no deviations from the test protocol experienced. One unresolved anomaly remains in the software. This anomaly seems to be minor and there are mitigations in place (phone communication) for this temporary issue. This is acceptable.

System Validation

The system level testing activities that were performed on the SW036 Remote Control software include system verification, validation and human factors testing.

System verification testing was performed on the Remote Control software with the purpose of verifying system level performance and features. System validation testing was performed to demonstrate that the Remote Control software meets the product user needs and intended uses per the product requirements specification and user labeling. Again, the three group approach described in the section above was used. The system V&V assesses the Remote Access Software and the OTS server application as a system (verification described in the section above assesses each of the components separately).

REVIEW COMMENTS: Testing verified that the system met requirements laid out in the system/finished device requirements. Testing was carried out by test, analysis, and review. All requirements had associated tests in one of these three categories. There were no design verification issues. All tests passed.

Testing validated (through bench testing) that user needs/intended uses are met through operational objectives of programmability and connectivity. This testing focused primarily on regression testing to ensure existing functionality is maintained. The sponsor tested the system to use scenarios regarding compatibility, use of desktop features, use of device application functions, installation, etc. and all tests passed. Anomaly inducement was also used to validate mitigations in place for hazardous situations. This testing is acceptable.

Two unresolved anomalies remain in the system. One of which was a disconnection during a remote support session, which seems to contradict the system requirement that the connection should be maintained throughout a session. A deficiency was sent to the sponsor and addressed in Amendment 1. The sponsor clarified that this anomaly occurred during the development phase of the system and did not occur during system verification testing. This response was found to be acceptable by the FDA review team.

Human Factors Testing

The primary objectives of the human factors testing were to:

- Validate the design of new or significantly changed functionality within the 2090 CareLink Programmer Remote Access system and ensure that it integrates well with the existing features and functionality of the RemoteView system
- Evaluate primary operating functions for representative usage scenarios identified during intended use research and assess if users can meet the success criteria
- Evaluate whether use errors that may cause potential harm have been mitigated to a satisfactory level

Test participants included fifteen (15) device nurses/technicians who are currently responsible for performing Medtronic device follow-ups acting as the remote operators (referred to as RTSPs). Fifteen (15) general cardiology practice nurses/certified cardiovascular technicians/or equivalent who have no or less than one year experience with the Medtronic programmer, are not responsible for performing device follow-ups, and are qualified to monitor and appropriately respond to cardiac symptoms acted as the local operators (referred to as LHCPs). The RTSPs received training on the overview of the system and use of the verbal protocol. LHCPs did not go through any training before the study.

It is important to note the following training inputs used for RTSP training. These represent real-life scenarios that may occur during use of the system. Remote technical users of the system will receive this training.

- Patient faints and falls (mitigation: Remote technical support provider instructs Local healthcare provider to ensure that patient is seated or lying down during follow-up procedure)
- Tests that are interrupted by network issues (mitigation: Local healthcare provider presses screen with touch pen as directed by Remote technical support provider)
- Changes in patient status (symptom related) that the Remote technical support provider cannot see (mitigation: Local healthcare provider communicates these to the Remote technical support provider via phone)
- Suspension of therapy by Remote technical support provider prevented by network issues (mitigation: Remote technical support provider communicates need to press VVI button (Emergency Hard Key) to Local healthcare provider)
- For tachycardia patients, Local healthcare providers, if untrained, are instructed by the Remote technical support provider during the introduction to the employ clinic resources to respond to a serious patient emergency.

The success criteria/usability goals for the study are outlined in the system requirements. Based on the results of the study, the sponsor concluded that:

- 100% of participants completed the study tasks with no uncorrected use errors that could result in a hazardous outcome

- All goals related to usability were achieved

On this basis, the sponsor believes this study demonstrates that the 2090 CareLink Programmer Remote Access System is, from a Human Factors perspective, safe and effective for use.

REVIEW COMMENTS: A human factors engineer was assigned a consult to review the testing described above during the first round of review. The engineer believed that the study was adequate. A deficiency was sent to the sponsor to inform them that, if significant changes were made on the system based on FDA's concerns with the verbal protocol and labeling, further human factors validation may be necessary. This was addressed by the sponsor in Amendment 1. FDA does not believe further testing is necessary and so the testing described above remains adequate.

Clinical Review

The sponsor did not provide any clinical data to support the Remote Control Software. Several FDA clinicians participated in discussions regarding this software and their perspectives are incorporated into this memo.

Wireless

There is no change to the method in which the 2090 Programmer accesses the OTS server application via the Internet as compared to the RemoteView Software Application. There is no change to the hardware or wireless connectivity of the 2090 Programmer. Therefore, the sponsor did not provide any wireless information or testing in this submission.

REVIEW COMMENTS: FDA believes it is acceptable for the sponsor to leverage wireless connectivity verification from the approved RemoteView software. The 2090 Programmer's wireless capability is approved. Cybersecurity controls are in place to protect the control of the programmer. This information is acceptable.

Cybersecurity

Medtronic has implemented system security for the proposed software according to FDA's Cybersecurity Guidance. Medtronic has established product security practices to address baseline risks and risks identified by the product security risk assessment. Secure design practices, including hazard identification, analysis, baseline security requirements, secure design controls, and secure implementation development and testing have been implemented for this system.

Per the Cybersecurity Guidance, the sponsor provides a specific list of cybersecurity risks that are traced to design requirements built into the system. The OTS server application system mitigates for many of these risks and has been verified and validated accordingly. The 2090 Programmer will remain free of malware as the 2090 Programmer network features are designed to only initiate outbound connections and do not accept incoming connections (local operator is responsible for inputting session key). Additionally, the 2090 Programmer is configured with a firewall that blocks unsolicited connections. Finally, the 2090 Programmer reverts to a known state upon every reboot, removing any malware that may have been present.

In terms of unauthorized (malicious) use of the system, the sponsor has incorporated mitigations to address this hazard. Again, the programmer user initiates all communications through an out-of-band mechanism. An attacker wishing to control a programmer would need to arrange for a programmer user to call them directly to generate the session token. The OTS server application also provides SSL authentication for all external connections.

Security of Data

The Remote Control software follows industry standard practices in preservation of confidentiality, integrity, availability, and accountability (CIAA) in protecting patient data and providing expected performance. These practices are focused on intrusion attempts from sources external to the Remote Control system. It should be noted that Remote Control data security features are identical to the data security features used for RemoteView and so the sponsor has not implemented any additional data security changes as a result of the inclusion of remote control access.

Confidentiality

The sponsor ensures confidentiality of data by the following protocols and controls: Secure Socket Layer (SSL) HTTPS, the OTS server application Cryptographic Engine (FIPS compliant), Automatic Session Termination, Unique Passcodes and User Credentials, Delivery of confidential passcode (over the telephone), and Identity of remote party is assured over the phone.

Integrity

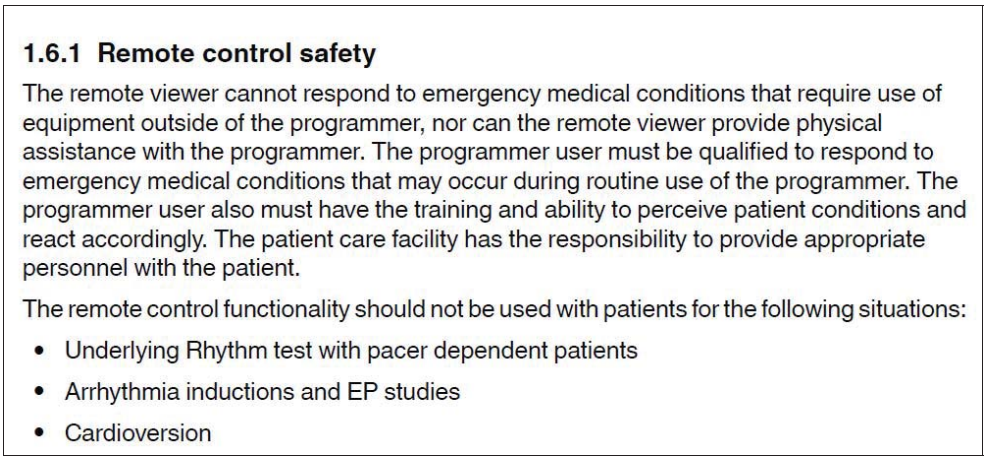
The integrity of the data being viewed has been validated and tested by the software validation process. Cryptographic authentication of the data communications also ensure that the data being shown on the Medtronic programmer is the same data that is viewed by the remote party.

REVIEW COMMENTS: Overall, the sponsor has presented an adequate approach to the cybersecurity of the system. Little has changed since approval of the system from remote viewing purposes previously. Because more serious risks are presented with remote control and further vulnerabilities are present in the system, the sponsor has adjusted the requirements accordingly. These requirements have been verified and validated in the system V&V described in previous sections of this memo. FDA has no further concerns with the sponsor's cybersecurity approach.

Labeling

The sponsor provided the following labeling associated with the Remote Control Software:

- Medtronic CareLink RemoteView Supplemental Manual – this manual explains the functionality of remote access software and includes a section on using the remote control feature. This section includes the following language as a warning against using the remote control feature in certain situations.



1.6.1 Remote control safety

The remote viewer cannot respond to emergency medical conditions that require use of equipment outside of the programmer, nor can the remote viewer provide physical assistance with the programmer. The programmer user must be qualified to respond to emergency medical conditions that may occur during routine use of the programmer. The programmer user also must have the training and ability to perceive patient conditions and react accordingly. The patient care facility has the responsibility to provide appropriate personnel with the patient.

The remote control functionality should not be used with patients for the following situations:

- Underlying Rhythm test with pacer dependent patients
- Arrhythmia inductions and EP studies
- Cardioversion

Figure 2: Manual Language

- Tip Cards
    - Conducting a remote device check – this tip card explains the steps that need to be taken by the local operator to set up and turn on the programmer, establish the phone connection with the remote operator, interrogate the device, etc.
    - Setting up the Medtronic Programmer – this tip card (intended to be used by the local operator) goes into further detail on setting up, powering, and connecting the 2090 Programmer
    - Remote device check procedure – this tip card is intended for the remote technical support provider and lists all steps that need to be taken before, during and after the remote session. This includes confirming the patient's identity, initiating the verbal protocol, instructions when disconnection occurs, and ending the remote session safely.
    - Starting a technical support session – this tip card is intended to be used by the remote technical support provider and instructs the provider on how to open the OTS server application software, generate the session key, start screen sharing and end the session.

REVIEW COMMENTS: Overall, the labeling and tip cards adhere to the sponsor's requirements for the system. For this system, these tip cards are one of the main risk controls used to mitigate identified hazards. The labeling and tip cards were validated in the human factors study. As stated previously, FDA had several concerns regarding the labeling and verbal protocol, which were reflected in the March 19, 2015 deficiency letter. These concerns were addressed during interactive discussions and in Amendment 1. The modifications proposed in Amendment 1 were found to be acceptable. See sections above for more information on changes made to the labeling and verbal protocol.

Conclusions/Recommendation

Several deficiencies were found during the review of the original supplement and a Major Deficiency Letter was sent to the sponsor on March 19, 2015. Through interactive discussions and in Amendment 1, responses to these deficiencies have been proposed by the sponsor and found to be acceptable by FDA. Overall, FDA believes that the risk controls implemented are adequate and address many of the concerns that FDA has had throughout the course of the review. Further guidance on the use of the Remote Control software may need to be developed by the medical community. FDA recommends approval of the Remote Control Software.