

## Model 3120 Programmer/Recorder/Monitor Operator's Manual

Enhancements have been made to the PRM's secure export feature. The following sections of the 3120 Operator's Manual have been updated:

- System Features
- Patient Data Management Features
- Export Data
- Transfer Data
- PRM Storage

### System Features

The option to encrypt patient data is an important system feature enabling the PRM user to protect patient data privacy and maintain security. The following statement was added to the list of System Features.

- Provides the option to encrypt patient data prior to exporting to a USB pen drive.

### Patient Data Management Features

The Patient Data Management utility allows the user to export, transfer, print, read, and delete patient data.

**Privacy Notice:** By exporting data from the PRM, you are assuming the responsibility for the privacy and security of that data. Printing, storing, transferring, reading, and deleting of patient data must be performed in compliance with applicable data privacy and security laws. Using the available secure export methods is recommended.

### Export Data

To provide flexibility for the PRM user while ensuring patient data security, the PRM now offers two options to export patient data to a USB pen drive. The following step supersedes step 4 in the **Export Data** section; use it within the context of the other steps in that section.

- To initiate export of the selected patient data, select the Export button. Patient data in plain format is neither encrypted nor compressed on the USB pen drive.
- To initiate export of the selected patient data with encryption, select the Export with Password Protection button. Password protection encrypts patient data on the USB pen drive.
  - When the system prompts you with the Initialize USB pen drive dialog box, enter and confirm a password. The password must be alpha numeric and contain at least six characters.
  - Select the Initialize button.

If the password does not meet system requirements, the system displays the Password Creation Failed dialog box and prompts you to try again.

When using a non-Boston Scientific computer (e.g., a clinic PC), enter your password to access encrypted patient data stored on the USB pen drive.

**NOTE:** The USB pen drive used to store exported patient data cannot simultaneously contain encrypted and non-encrypted patient data.

### Transfer Data

The steps below clarify how the PRM transfers patient data to a USB pen drive. The PRM uses different file naming conventions based on whether data is encrypted. Refer to the **Transfer Data** section of the Operator's Manual.

Each patient record on the USB pen drive is stored in a folder with the following naming conventions:

- For non-encrypted patient data, the patient folder name appears in this format:  
<last name>-<first name>-<birth date>-<model>-<serial>
- For encrypted patient data, the patient folder name appears in this format:  
<model>-<serial>

The **Export Data** operation transfers the most recent patient data from the PRM to the USB pen drive. It also moves the patient data from the previous sessions to the "old" subfolder within the same patient folder on the USB pen drive.

### PRM Storage

The user must maintain patient data security when transferring patient data to floppy disks. The change below enhances the original statement in the **PRM Storage** section to emphasize floppy disk security.

- If using a patient data disk, remove the disk from the disk drive, and store the disk in a safe place. You are responsible for the security of this disk and the associated patient data.



**Manufacturer**  
Boston Scientific  
4100 Hamline Avenue North  
St. Paul, MN 55112-5798 USA

www.bostonscientific.com

1.800.CARDIAC (227.3422)

+1.651.582.4000

© 2012 Boston Scientific or its affiliates.  
All Rights Reserved.



359065-002 EN US 2012-12

