Product Security White Paper

Arctic Sun™ Stat Temperature Management System

BD is committed to providing secure products to our customers given the important benefits they provide to patient health. We value the confidentiality, integrity and availability of all information, including protected health and personally identifiable information (e.g. PHI, PII, and other types of personal data and sensitive data) and are committed to comply with applicable regional, federal and local privacy and security laws and regulations, including the Health Insurance Portability, Accountability Act (HIPAA), and the General Data Protection Regulation.

BD has implemented reasonable administrative, technical and physical safeguards to help protect against security incidents and privacy breaches involving a BD product, provided those products are used in accordance with BD’s instructions for use. However, as systems and threats evolve, no system can be protected against all vulnerabilities and we consider our customers the most important partner in maintaining security and privacy safeguards. If you have any concerns, we ask that you bring them to our attention, and we will investigate. Where appropriate, we will address the issue with product changes, technical bulletins and/or responsible disclosures to customers and regulators. BD continuously strives to improve security and privacy throughout the product lifecycle using practices such as:

- Privacy and Security by Design
- Product and Supplier Risk Assessment
- Vulnerability and Patch Management
- Secure Coding Practices and Analysis
- Vulnerability Scanning and Third-Party Testing
- Access Controls appropriate to Customer Data
- Incident Response
- Clear paths for two-way communication between customers and BD

If you would like to report a potential product related privacy or security issue (incident, breach or vulnerability), please contact the BD Product Security team:

Site:  http://www.bd.com/productsecurity/
Email: ProductSecurity@bd.com

Mail:

  Becton, Dickinson and Company
  Attn: Product Security
  1 Becton Drive
  Franklin Lakes, New Jersey 07417-1880

The purpose of this document is to detail how our security and privacy practices have been applied to the Arctic Sun™ Stat Temperature Management System, what you should know
about maintaining security of this product and how we can partner with you to ensure security throughout this product’s lifecycle.

Contents

Product Description .................................................................................................................................................. 3
Hardware Specifications ........................................................................................................................................ 3
Operating Systems .............................................................................................................................................. 3
Third-party Software ........................................................................................................................................... 3
Network Ports and Services ............................................................................................................................... 3
Sensitive Data Transmitted .................................................................................................................................. 3
Sensitive Data Stored ........................................................................................................................................ 3
Network and Data Flow Diagram ...................................................................................................................... 4
Malware Protection ............................................................................................................................................. 4
Patch Management ............................................................................................................................................. 4
Authentication Authorization .............................................................................................................................. 4
Network Controls ................................................................................................................................................ 4
Encryption .......................................................................................................................................................... 4
Audit Logging ..................................................................................................................................................... 5
Remote Connectivity ......................................................................................................................................... 5
Service Handling .............................................................................................................................................. 5
End-of-Life and End-of-Support ........................................................................................................................ 5
Secure Coding Standards ................................................................................................................................... 5
System Hardening Standards ............................................................................................................................. 5
Risk Summary .................................................................................................................................................. 5
Third Party Soc2+ Reporting ............................................................................................................................. 5
Manufacturer’s Disclosure Statement for Medical Device Security ............................................................... 6
Disclaimer ........................................................................................................................................................ 12
Product Security White Paper Signature Approval Form ............................................................................... Error! Bookmark not defined.
**Product Description**

The Arctic Sun™ Stat Temperature Management System Temperature Management System is a non-invasive, thermal regulating system, indicated for monitoring and controlling patient temperature. The system is composed of the Arctic Sun™ Stat Temperature Management System Control Module and disposable non-sterile ArcticGel Pads, which are adhered to areas of the patient’s skin. The Control Module is the device that contains software. The ArcticGel Pads do not contain software or any sensors.

The Arctic Sun™ Stat Temperature Management System’s Control Module re-circulates temperature-controlled water to the ArcticGel Pads. A commercially-available medical temperature probe, such as naso-pharyngeal, bladder, rectal, or esophageal, connected to the control module senses the patient’s core temperature. Within the device, a control algorithm automatically adjusts the water temperature (automatic mode) or the clinician can adjust the water temperature (manual mode) to obtain the desired patient temperature.

**Hardware Specifications**

- 10.4" XGA/SVGA TFT LCD display with LED backlight
- Intel® Celeron® processor N3060
- USB 3.0

**Operating Systems**

Microsoft Windows 10 LTSC

**Third-party Software**

- Microsoft Windows 10 LTSC
- Veracrypt
- Cylance Protect

**Network Ports and Services**

- User settable; Full range output
- CCE connection (for Encrypted data transfer to EMR)

**Sensitive Data Transmitted**

There is no sensitive data in transit. Patient data in transit consists only of the patient’s temperature with no additional identifiable information.

**Sensitive Data Stored**

No sensitive data is stored.
Network and Data Flow Diagram

Malware Protection
CylanceProtect is being used.

Patch Management
BD approved upgrades can be applied to the device. This requires BD personal to update at the site.

Authentication Authorization
None, the Arctic Sun™ Stat Temperature Management System is a local device only.

Network Controls
There are no network controls that need to be implemented by the user.

Encryption
No sensitive data is handled by application. If encryption on a USB software update fails, a failure symbol is displayed to the user.
Audit Logging
An internal log store can only be exported by developers; there is no concept of users with this system. Alarm logs can be viewed, however, there is no exportability. Error logs are limited in access to the same elevated mode needed to adjust calibration settings. Authorization is tied to authorization of product use.

Remote Connectivity
There is no remote connectivity for the Arctic Sun™ Stat Temperature Management System.

Service Handling
Following installation and configuration Arctic Sun™ Stat Temperature Management System is designed to operate without service user interaction for up to 6 months of calendar time wherein calibration is required.

End-of-Life and End-of-Support
BD follows an internal process to provide end-of-life and end-of-support notifications directly to customers, where appropriate. Currently there is no plan for end-of-life or end-of-support for this device and/or service.

Secure Coding Standards
Secure coding standards have not been applied.

System Hardening Standards
Hardening standards have been applied to the operating system.

Risk Summary
A penetration test was performed on the Arctic Sun™ Stat Temperature Management System and was found to have a LOW CVSS rating. If a potential vulnerability is discovered or other potential security risk identified, BD will take all reasonable measures to address the issue and update this risk summary.

Third Party Soc2+ Reporting
Our commitment to ongoing Service Organization Control (SOC) Type II Plus reporting enhances the transparency of our relationship with customers. This reporting allows for visibility into the policies, procedures and processes governing the use of data gathered from customer environments.

Using an independent third party, we annually test and report on the operating effectiveness of controls in relation to the trust services principles & criteria for security and availability, as well as NIST800-66 (An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule). The third party firm completes their reporting in alignment with the American Institute of Certified Public Accountants (AICPA) over the suitability of the design and operating effective of controls to meet the applicable criteria.
As part of this review, the following areas will be assessed:

1. Security Management Process
2. Security Official
3. Workforce Security
4. Information Access Management
5. Security Awareness and Training
6. Security Incident Procedures
7. Contingency Plan
8. Evaluation
9. Business Associate Contracts and Other Arrangements
10. Facility Access Controls
11. Workstation Use
12. Workstation Security
13. Device and Media Controls
14. Access Controls
15. Report Controls
16. Integrity
17. Person or Entity Authentication
18. Transmission Security
19. Business Associate Monitoring Process
20. Policies and Procedures

**Manufacturer’s Disclosure Statement for Medical Device Security**

Otherwise known as the MDS2 form, this section provides an industry standard convention for security information.
**MANUFACTURER DISCLOSURE STATEMENT FOR MEDICAL DEVICE SECURITY – MDS²**

**DEVICE DESCRIPTION**

<table>
<thead>
<tr>
<th>Device Category</th>
<th>Manufacturer</th>
<th>Document ID</th>
<th>Document Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted Temperature Management</td>
<td>BD (Becton, Dickinson and Company)</td>
<td>DCS-28-5741-0061</td>
<td>2020-05-08</td>
</tr>
<tr>
<td>Device Model</td>
<td>Software Revision</td>
<td>Software Release Date</td>
<td></td>
</tr>
<tr>
<td>Arctic Sun™ Stat Temperature Management System</td>
<td>V1.0.4</td>
<td>2020-06-12</td>
<td></td>
</tr>
</tbody>
</table>

**Manufacturer or Representative Contact Information**

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Manufacturer Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BD (Becton, Dickinson and Company)</td>
<td>Becton, Dickinson and Company</td>
</tr>
<tr>
<td>Representative Name/Position</td>
<td>Attn: Product Security and Privacy</td>
</tr>
<tr>
<td>1-800-531-4140</td>
<td>1 Becton Drive, Franklin Lakes, New Jersey 07417-1880</td>
</tr>
</tbody>
</table>

**Intended use of device in network-connected environment:**

The intended use of the Arctic Sun™ Stat Temperature Management System is a tool to manage patients’ temperature. The Arctic Sun™ Stat Temperature Management System helps create, store, or transfer the temperature data for record keeping purposes. It also helps have easy access to information related to health conditions and to communicate information that could be reviewed for determination of potential medical conditions to their healthcare provider.

**Intended purpose of integrating the Device into an IT-Network: EMR Charting**

**MANAGEMENT OF PRIVATE DATA**

Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.

<table>
<thead>
<tr>
<th>A</th>
<th>Can this device display, transmit, or maintain private data (including electronic Protected Health Information [ePHI])?</th>
<th>Yes, No, N/A or See Note</th>
<th>Note #</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Types of private data elements that can be maintained by the device:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.1</td>
<td>Demographic (e.g., name, address, location, unique identification number)?</td>
<td>No</td>
<td>1,2</td>
</tr>
<tr>
<td>B.2</td>
<td>Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>B.3</td>
<td>Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>B.4</td>
<td>Open, unstructured text entered by device user/operator?</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>B.5</td>
<td>Biometric data?</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>B.6</td>
<td>Personal financial information?</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**C |** Maintaining private data - Can the device:

| C.1 | Maintain private data temporarily in volatile memory (i.e., until cleared by power-off or reset)? | No | |
| C.2 | Store private data persistently on local media? | No | |
| C.3 | Import/export private data with other systems? | No | |
| C.4 | Maintain private data during power service interruptions? | No | |

**D |** Mechanisms used for the transmitting, importing/exporting of private data – Can the device:

| D.1 | Display private data (e.g., video display, etc.)? | No | |
| D.2 | Generate hardcopy reports or images containing private data? | No | |
| D.3 | Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)? | No | |
| D.4 | Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)? | No | |
| D.5 | Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)? | No | |
| D.6 | Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)? | No | |
| D.7 | Import private data via scanning? | No | |
| D.8 | Other? | N/A | |

Management of private data notes:

1. Device does not have the ability to gather, display, or maintain private data.
2. Device does not have the ability to generate hardcopy or retrieve any private data.
<table>
<thead>
<tr>
<th>Device Category</th>
<th>Manufacturer</th>
<th>Document ID</th>
<th>Document Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arctic Sun™ Stat Temperature Management System</td>
<td>BD (Becton, Dickinson and Company)</td>
<td>N/A</td>
<td>2020-05-08</td>
</tr>
</tbody>
</table>

### SECURITY CAPABILITIES

Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.

| 1 | AUTOMATIC LOGOFF (ALOF) | **No** | 1 |

- **1-1** Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?

  - **1-1.1** Is the length of inactivity time before auto-logoff/session lock user or administrator configurable? (Indicate time in notes.)

  - **1-1.2** Can auto-logoff/session lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user?

- **ALOF notes:**
  1. Device does not utilize user log-in function to allow usage of the equipment, identify user, or to provide user lockout function.

| 2 | AUDIT CONTROLS (AUDT) | **No** | N/A |

- **2-1** Can the medical device create an audit trail?

  - **2-2** Indicate which of the following events are recorded in the audit log:

  - **2-2.1** Login/logout
  - **2-2.2** Display/presentation of data
  - **2-2.3** Creation/modification/deletion of data
  - **2-2.4** Import/export of data from removable media
  - **2-2.5** Receipt/transmission of data from/to external (e.g., network) connection
  - **2-2.5.1** Remote service activity
  - **2-2.6** Other events? (describe in the notes section)

- **AUDT notes:**
  1. Device, by design, does not track events, or track user events and record in a log file to create an audit trail of activity.

| 3 | AUTHORIZATION (AUTH) | **No** | 1 |

- **3-1** Can the device prevent access to unauthorized users through user login requirements or other mechanism?

- **3-2** Can users be assigned different privilege levels within an application based on ‘roles’ (e.g., guests, regular users, power users, administrators, etc.)?

- **3-3** Can the device owner/operator obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?

- **AUTH notes:**
  1. Device does not utilize user log-in function to allow usage of the equipment, or to identify the user, or to assign differing levels of usage privilege or authorization.
### Rules of Use for IDMS 2.0.4

Refer to Section 2.3. of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Yes, No, N/A, or See Note</th>
<th>Note #</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><strong>CONFIGURATION OF SECURITY FEATURES (CNFS)</strong>&lt;br&gt;The ability to configure/re-configure device security capabilities to meet users’ needs.</td>
<td></td>
</tr>
<tr>
<td>4-1</td>
<td>Can the device owner/operator reconfigure product security capabilities?</td>
<td>No</td>
</tr>
<tr>
<td>CNFS notes:</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><strong>CYBER SECURITY PRODUCT UPGRADES (CSUP)</strong>&lt;br&gt;The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device’s security patches.</td>
<td></td>
</tr>
<tr>
<td>5-1</td>
<td>Can relevant OS and device security patches be applied to the device as they become available?</td>
<td>Yes</td>
</tr>
<tr>
<td>5-1.1</td>
<td>Can security patches or other software be installed remotely?</td>
<td>No</td>
</tr>
</tbody>
</table>
| CSUP notes: | 1. BD approved upgrades can be applied to the device. This requires BD personal to do such and is not directly available to customers.  
2. System does not provide ability of remote connection into the device for control. |
<p>| 6 | <strong>HEALTH DATA IDENTIFICATION (DIDT)</strong>&lt;br&gt;The ability of the device to directly remove information that allows identification of a person. |
| 6-1 | Does the device provide an integral capability to de-identify private data? | No |
| DIDT notes: | 1. The device does not collect or store any private data. |
| 7 | <strong>DATA BACKUP AND DISASTER RECOVERY (DTBK)</strong>&lt;br&gt;The ability to recover after damage or destruction of device data, hardware, or software. |
| 7-1 | Does the device have an integral data backup capability (i.e., backup to remote storage or removable media such as tape, disk)? | No |
| DTKB notes: | 1. Device is not equipped with or design to provide backup functionality as private data is not collected or stored. |
| 8 | <strong>EMERGENCY ACCESS (EMRG)</strong>&lt;br&gt;The ability of device users to access private data in case of an emergency situation that requires immediate access to stored private data. |
| 8-1 | Does the device incorporate an emergency access (&quot;break-glass&quot;) feature? | No |
| EMRG notes: | 1. The device does not collect or store any private data. |
| 9 | <strong>HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)</strong>&lt;br&gt;How the device ensures that data processed by the device has not been altered or destroyed in an unauthorized manner and is from the originator. |
| 9-1 | Does the device ensure the integrity of stored data with implicit or explicit error detection/correction technology? | No |
| IGAU notes: | 1. The device does not employ any additional means and measures against data integrity as no private data are gathered, processed, or manipulated |</p>
<table>
<thead>
<tr>
<th>Device Category</th>
<th>Manufacturer</th>
<th>Document ID</th>
<th>Document Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile app</td>
<td>BD (Becton, Dickinson and Company)</td>
<td>N/A</td>
<td>2020-05-08</td>
</tr>
<tr>
<td>Device Model</td>
<td>Arctic Sun™ Stat Temperature Management System</td>
<td>V1.0.4</td>
<td>2020-06-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Refer to Section 2.3.2.3 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.

### 10 MALWARE DETECTION/PROTECTION (MLDP)

The ability of the device to effectively prevent, detect and remove malicious software (malware).

10-1 Does the device support the use of anti-malware software (or other anti-malware mechanism)? ............... Yes 1

10-1.1 Can the user independently re-configure anti-malware settings? .............................................. No

10-1.2 Does notification of malware detection occur in the device user interface? ................................. No

10-1.3 Can only manufacturer-authorized persons repair systems when malware has been detected? ....... Yes

10-2 Can the device owner install or update anti-virus software? ................................................................. No

10-3 Can the device owner/operator (technically/physically) update virus definitions on manufacturer-installed anti-virus software? ................................................................. No 2

MLDP notes:
1. Cylance Protect is the anti-malware application used.
2. Cylance Protect does not use virus definitions, it is an AI and machine learning based system.

### 11 NODE AUTHENTICATION (NAUT)

The ability of the device to authenticate communication partners/nodes.

11-1 Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information? ................................. No

NAUT notes: N/A

### 12 PERSON AUTHENTICATION (PAUT)

Ability of the device to authenticate users.

12-1 Does the device support user/operator-specific username(s) and password(s) for at least one user? ............ No 1

12-1.1 Does the device support unique user/operator-specific IDs and passwords for multiple users? ............ No 1

12-2 Can the device be configured to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)? ................................................................. No 1

12-3 Can the device be configured to lock out a user after a certain number of unsuccessful logon attempts? ...... No 1

12-4 Can default passwords be changed at/prior to installation? ................................................................. No 1

12-5 Are any shared user IDs used in this system? ......................................................................................... No 1

12-6 Can the device be configured to enforce creation of user account passwords that meet established complexity rules? ......................................................................................... No 1

12-7 Can the device be configured so that account passwords expire periodically? .................................... No 1

PAUT notes: 1. Device does not utilize user log-in function to allow usage of the equipment, or to identify the user.

### 13 PHYSICAL LOCKS (PLOK)

Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of private data stored on the device or on removable media.

13-1 Are all device components maintaining private data (other than removable media) physically secure (i.e., cannot remove without tools)? ................................................................. N/A 1

PLOK notes: 1. Device does not collect or store any private data.
<table>
<thead>
<tr>
<th>Device Category</th>
<th>Mobile app</th>
<th>Manufacturer</th>
<th>Document ID</th>
<th>Document Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>BD (Becton, Dickinson and Company)</td>
<td>N/A</td>
<td>2020-05-08</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Model</th>
<th>Arctic Sun™ Stat Temperature Management System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Revision</td>
<td>V1.0.4</td>
</tr>
<tr>
<td>Software Release Date</td>
<td>2020-06-12</td>
</tr>
</tbody>
</table>

Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.

**14 ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)**

Manufacturer's plans for security support of 3rd party components within device life cycle.

14-1 In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).

14-2 Is a list of other third party applications provided by the manufacturer available? See Note

1. Windows 10 Enterprise LTSB 2016 64-bit Build 14393
2. Cylance Version 2.0.1510.10
3. VeraCrypt Version 1.23

**15 SYSTEM AND APPLICATION HARDENING (SAHD)**

The device's resistance to cyber attacks and malware.

15-1 Does the **device** employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards. Yes 1

15-2 Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update? Yes

15-3 Does the **device** have external communication capability (e.g., network, modem, etc.)? Yes

15-4 Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)? N/A

15-5 Are all accounts which are not required for the **intended use** of the **device** disabled or deleted, for both users and applications? Yes

15-6 Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device** disabled? Yes

15-7 Are all communication ports which are not required for the **intended use** of the **device** closed/disabled? Yes

15-8 Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the **intended use** of the **device** deleted/disabled? Yes

15-9 Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the **intended use** of the **device** deleted/disabled? Yes

15-10 Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)? No

15-11 Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools? No

**SAHD notes:**

1. DISA STIG per BD policy

**16 SECURITY GUIDANCE (SGUD)**

The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service.

16-1 Are security-related features documented for the **device user**? No 1

16-2 Are instructions available for **device/media sanitization** (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)? No 1

**SGUD notes:**

1. The device does not have any interface for security changes to be made by the device user.
**Device Category** | **Manufacturer** | **Document ID** | **Document Release Date**
--- | --- | --- | ---
Mobile app | BD (Becton, Dickinson and Company) | N/A | 2020-05-08

**Device Model** | **Software Revision** | **Software Release Date**
Arctic Sun™ Stat Temperature Management System | V1.0.4 | 2020-06-12

Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.

### HEALTH DATA STORAGE CONFIDENTIALITY (STCF)
The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of private data stored on device or removable media.

<table>
<thead>
<tr>
<th>17-1 Can the device encrypt data at rest?</th>
<th>Yes, No, N/A, or See Note</th>
<th>Note</th>
</tr>
</thead>
</table>

STCF notes: 1. While the device does not collect or store any private data, the system does use a TPM and bitlocker.

### TRANSMISSION CONFIDENTIALITY (TXCF)
The ability of the device to ensure the confidentiality of transmitted private data.

| 18-1 Can private data be transmitted only via a point-to-point dedicated cable? | No | 1 |
| 18-2 Is private data encrypted prior to transmission via a network or removable media? If yes, indicate in the notes which encryption standard is implemented. | No | 1 |
| 18-3 Is private data transmission restricted to a fixed list of network destinations? | No | 1 |

TXCF notes: 1. The device does not collect or store any private data.

### TRANSMISSION INTEGRITY (TXIG)
The ability of the device to ensure the integrity of transmitted private data.

| 19-1 Does the device support any mechanism intended to ensure data is not modified during transmission? | No |

TXIG notes: N/A

### OTHER SECURITY CONSIDERATIONS (OTHR)
Additional security considerations/notes regarding medical device security.

| 20-1 Can the device be serviced remotely? | No |
| 20-2 Can the device restrict remote access to/from specified devices or users or network locations (e.g., specific IP addresses)? | No |
| 20-2.1 Can the device be configured to require the local user to accept or initiate remote access? | No |

OTHER Notes: N/A

---

**Disclaimer**
The information contained in this Product Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify or supersede the terms and conditions of any written agreement between such customer and BD, or BD’s subsidiaries or affiliates (collectively, “BD”). BD does not make any promises or guarantees to customer that any of the methods or suggestions described in this Product Security White Paper will restore customer’s systems, resolve any issues related to any malicious code or achieve any other stated or intended results. Customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security White Paper, and customer agrees to indemnify and hold BD harmless from the same.