Product Security White Paper

BD Remote Support Services (RSS)

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 EC 95/46 Directive.

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 BD Remote Support Services, 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

The BD Remote Support Services (RSS) solution is a support platform built for remotely managing the BD-developed products that are deployed to facilities that BD customers own and operate, as well as products hosted by BD. The BD Remote Support Services Platform is comprised of components that perform the following major functions:

- Remote Access
- Remote Monitoring **
- Remote Package Deployment **
- Remote Management of Microsoft Patches
- Remote Management of Antivirus **
- Customer Audit Reports **
- Remote software installation and configuration **

** Features exist for non-Department of Defense (DOD) customers.

All of the functions of the RSS Platform are performed through an interactive web application.

BD Remote Support Services (RSS) is a scalable cloud-based platform for BD to effectively launch and manage products deployed around the globe.

- Minimizes product downtime through remote management and proactive monitoring.
- Simplify product implementation through integrated mass software updates.
- Manage product security compliance

Hardware Specifications

- RSS and Remote Implementation Platform:
  - Hosted in Microsoft Azure
  - BD is responsible for maintaining the RSS platform
- Bomgar Infrastructure
  - Hosted and managed by BD
- RSS and Remote Implementation Agent
  - Product specific (See Products Types Supported section)

Operating Systems

- RSS Platform
  - Microsoft Azure Server 2012 Data Center
- RSS and Remote Implementation Agent (See product specific documentation for supported operating systems)
  - Windows Server 2016
  - Windows Server 2012/2012 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2003
  - Windows XP
  - Windows 7
  - Windows 10
  - Windows XP embedded
  - Windows 7 Embedded
- Bomgar
  - Windows Server 2016
  - Windows Server 2012/2012 R2
  - Windows Server 2008/2008 R2
  - Windows 7
  - Windows 10
  - Windows 7 Embedded
- Bomgar Jump Client
  - Windows Server 2000
  - Windows 2000 professional
  - Windows Server 2003 (SP1)
  - Windows XP SP2 and below

Third-party Software

RSS Agent

- Sqlite
- Vistadb
- Sql Server Compact.NET 4.0 and above, requires a full version. The RSS Platform is built using Microsoft Azure cloud services. These services include:

Microsoft Azure Web services:

- Microsoft Azure Databases
- Microsoft Azure Identity
- Microsoft Azure Networking
- Microsoft Azure Storage
- Microsoft Azure Security

Network Ports and Services

- All communication out of Hospital network is done through port 443
- Package metadata for WSUS transmitted over port 80
- Data received into the Hospital network is done through port 443

Department of Defense only: DOD specific infrastructure for WSUS and Bomgar communication remain the same. There is no outbound traffic from RSS Agents for the purpose of monitoring and package deployment.

Sensitive Data Transmitted

RSS does not pull any ePHI as a part of routine support procedures. In the event RSS collects any sensitive data from a device while service is being performed, it transmits information over a secure connection and maintains it on an encrypted data store. The RSS system only retains this type of data for the duration of the support engagement. BD will sign an appropriate HIPAA Business Associates Agreements (BAA) with customers for whom it accesses, upon request.

Remote screen sharing sessions have the potential to display the following information on a support technicians' desktop:

- Demographics (e.g., name, address, Date of birth, location, unique identification number)
- Medical record (e.g., medical record #, account #, test or treatment date, device identification number).

This information is not recorded or stored by RSS.

NOTE: The Validation tool compares and sends differences in HL7 and CMS2 messages transferred over https which may contain the following sensitive data transmitted:

- Demographics (e.g., name, address, Date of birth, location, unique identification number)
- Medical record (e.g., medical record #, account #, test or treatment date, device identification number).

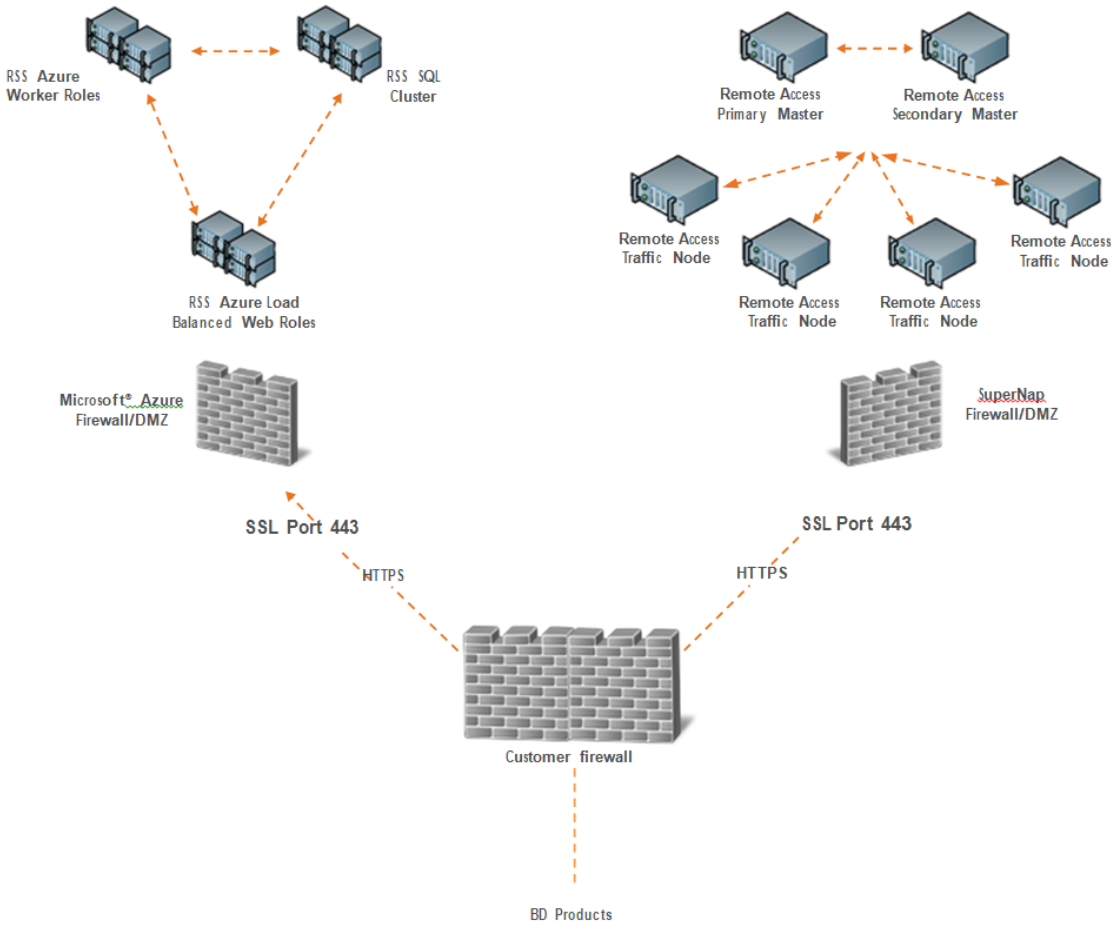
Sensitive Data Stored

The Validation tool compares and sends differences in HL7 and CMS2 messages. Messages are stored and encrypted on Microsoft Azure blob storage. The following sensitive data may be stored:

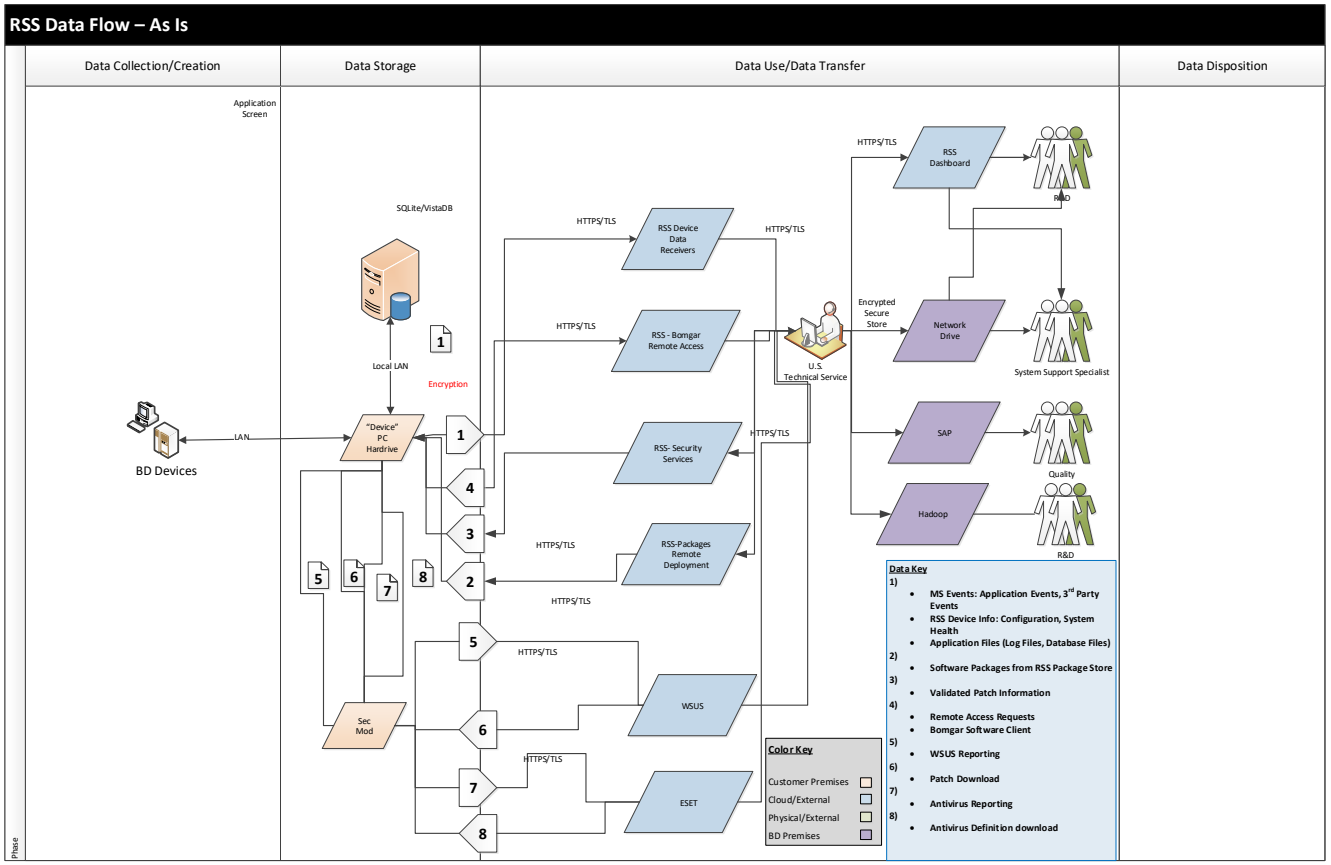
- Demographics (e.g., name, address, Date of birth, location, unique identification number) Medical record (e.g., medical record #, account #, test or treatment date, device identification number).

Network and Data Flow Diagram

BD Remote Support Services and Automate Remote Installation and Administration (ARIA) Network Architecture

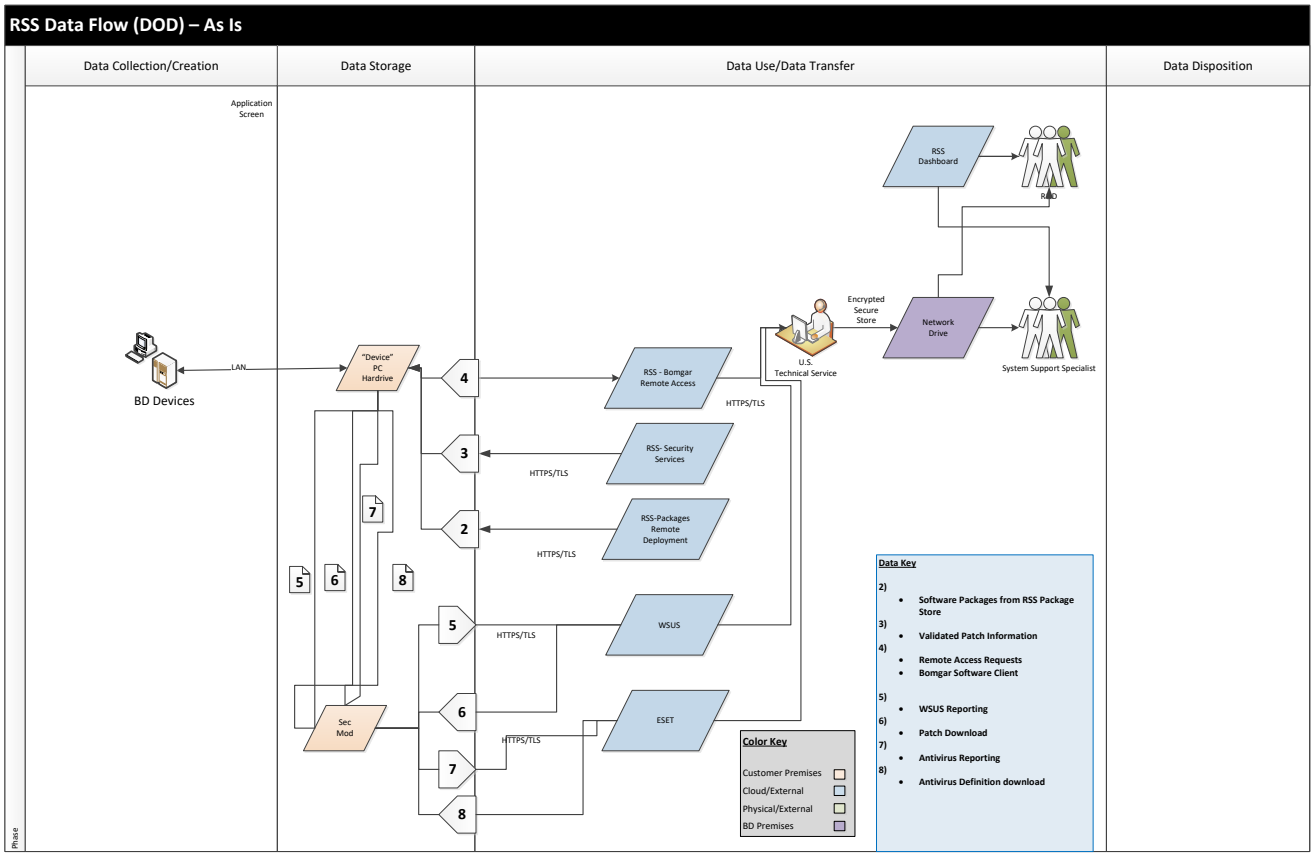


Commercial Customers



[Space Intentionally Left Blank]

Department of Defense (DOD) Customers



Malware Protection

RSS offers the Security Compliance Solution. This solution enables the BD support organization to proactively monitor and manage patching and security compliance of the BD installed base. The RSS Security Compliance Solution delivers the following key functionalities for BD support users:

- Patch management:
  - Ability to centrally manage the scheduling, testing, and deployment of Microsoft patches through a consistent and automated workflow
- NOTE: Patch management configuration for enabling automatic installation, reboots, and update time are discussed during implementation. See BD Supported Products for applicable productsActionable reports:
  - Security Compliance reports per device that provide insight into missing patches and count, as well as Windows Update Services (WSUS) and ESET anti-virus configuration information
  - White list / Blacklist reports that provide insight into Microsoft patches that are approved for installation per device type (White list) and those that are not approved for installation (Blacklist)

Hence, the RSS Security Compliance Solution enables the BD support personnel to proactively monitor and act to help ensure patching compliance of BD devices to minimize security vulnerabilities and share actionable information (e.g. Compliance reports) with BD customers.

The RSS Security Compliance Solution requires the RSS Security Component to run on the device in addition to the RSS Agent that provides remote support (i.e. remote access, monitoring, and updates) capabilities. This Security Component is rigorously tested and qualified before it is deployed to the BD device. The Security Component is remotely deployed to the device except in a break/fix scenario where it is manually installed along with the RSS Agent.

RSS Updates:
The status and operational health of BD products are continually addressed through BD RSS update services. New updates can be remotely installed to minimize the impact to customer operations. BD releases software updates in response to identified product needs. RSS provides customer operations the ability to customize the deployment schedule to minimize service disruptions.

In many cases, RSS update services have been incorporated into new BD products, for a more seamless update workflow. This level of integration ensures BD devices are not down for maintenance when they are needed most.

DOD Antivirus:
The Security Compliance Solution is not used in the DOD environment; instead, HBSS is used for performing Antivirus protection on BD devices.

Patch Management

Windows Security Updates are applied via WSUS. Monthly patch updates are reviewed and tested before being approved for deployment by each of the platforms supported via RSS. Upon approval, BD works with individual facilities to coordinate the deployment of the patches for each of the platforms. Patch management configuration for enabling automatic installation, reboots, and update time are discussed during implementation. See BD Supported Products for applicable products

A master Security Module WSUS/ESET server is connected to the Microsoft WSUS server and ESET distribution server. The approved updates metadata along with the corresponding updates are pulled down to these master servers. BD regional WSUS and ESET servers are connected to the BD master servers to receive approved updates metadata and corresponding updates. Security Module servers are connected to the regional servers to receive updates metadata and corresponding updates. Endpoint devices are then connected to the Security Module servers to receive updates.

DOD:
HBSS is installed, but not managed by BD.

Authentication Authorization

RSS authenticates BD users against a Microsoft® Active Directory instance that is maintained by BD. By using Active Directory, the RSS Enterprise dashboard authenticates users via a central, real-time LDAP authentication store. By utilizing this authentication method, the system maintains unique user credentials, requires strict password protocols and enforces periodic password changes. This method eliminates the need to maintain multiple sets of user information and the need for the enterprise and the device to store and manage external user passwords or other information. As a result, BD users who need access must first obtain a BD account via an employee onboarding process. Once a new BD employee has been granted an account, their direct management must provide additional training—including electronic PHI (ePHI) handling and authorization before they receive access to RSS. BD maintains an audit log of all BD users who have been granted access and completed the appropriate training. In the event that a BD employee leaves, BD suspends their account as a part of its standard off-boarding procedures.

Department of Defense(DOD) customers are not applicable and leverage separate authentication for Remote access into BD devices.

In addition, BD users working off-site require multi-factor authentication through a secure VPN connection in order to access RSS on the BD network.

RSS Customer Portal:

Users must be granted permissions by the facility through a registration and onboarding process that validates the registration information provided.

Remote Access Authorization:
Through RSS Customer Portal, customers are provided an additional layer of control by optionally requiring a secondary approval of remote access requests. This method can be useful for sensitive devices that customers want more visibility to whom and when devices are being accessed.

Patching approval:
Patching approval is tested and released through a controlled process managed through the RSS portal. RBAC is applied at each level and allows for auditing and security of the patch management process.

Network Controls

Most devices connected to the internet are not directly addressable from outside of the organization. To prevent security breaches, network administrators prefer that their computers and devices be hidden from the outside world behind secure firewalls, routers and proxy servers. This enables users within the facility to access the internet while aggressively preventing outside persons or applications from gaining visibility or access to the computers within the facility.

BD access to devices at the facility is restricted to BD devices running RSS Agents. RSS works within these boundaries by using a communication pattern that permits remote devices to exchange information with hosted RSS enterprise servers, even when devices are behind corporate firewalls or proxy servers. This technology for device-initiated communications is based on standard Hypertext Transfer Protocol Secure (HTTPS). With RSS, remote devices initiate all communications with an enterprise server at a globally visible address. This enables devices to be deployed in many environments without requiring any modification of security settings within the local network environment. As a result, if a web browser can access the internet using a TLS 1.2 network connection, the RSS-enabled device will be able to perform two-way communications with the enterprise server using the same network connection. This method of communication:

- Leverages the existing security infrastructure at the device location. The device receives the same network security coverage as all other computers within your facility.
- Simplifies device deployment. Your local IT staff often does not need to make any changes to their existing security configuration. When they connect the device to the local network, it is ready to communicate.

  Note: For facilities that employ web filtering, the RSS servers should be white-listed for proper operation.

- Inherently secures the device from attack. Since the device initiates all communication only to a specified server and does not possess a public IP address, an attacker has little opportunity to exploit the communication to gain access to the device.
- Our solution offers the possibility for egress filtering, the practice of monitoring and potentially restricting the flow of information outbound from one network to another.

The BD Technical Support Center does not share login accounts for remote support. Each user has a unique account into the RSS platform. The password is based on the BD Active Directory and is changed every 90 days or more frequently. The application uses an industry standard encryption to store and transmit all user passwords. BD requires a minimum of eight (8) characters for the password length and synchronizes all users with BD Active Directory, known as Lightweight Directory Access Protocol (LDAP). RSS permits three failed login attempts before the user is locked out for 30 minutes.

NOTE: Department of Defense(DOD) customers are not applicable as RSS agents are not installed

Encryption

All communication by RSS happens via Transport Layer Security (TLS) over TCP port 443 (outbound rule only). The RSS Dashboard supports TLS versions 1.2 – 1.0 starting with 1.2 based on client configuration. The RSS agent negotiates the connection protocol with the RSS Dashboard based on local OS settings which will vary based on the BD product. Remote access sessions made into remoteaccess-rss.carefusion.com are established using TLS 1.2.

The RSS TLS tunnel leverages industry standard ciphers negotiated between the remote device and the hosted BD RSS services.

RSS.carefusion.com = SHA256 with RSA 20148 bit/TLS 1.2
Aria.carefusion.com = SHA256 with RSA 20148 bit/TLS 1.2
Aria-api.carefusion.com = SHA256 with RSA 20148 bit/TLS 1.2
Remoteaccess-rss.carefusion.com = SHA256 with RSA 20148 bit/TLS 1.2
Install portal = SHA256 with RSA 20148 bit/TLS 1.2

DOD:
Bomgar clients communicate with the Bomgar server using SHA1 encryption.

Audit Logging

The RSS enterprise server electronically logs user identification, date and time, and device ID anytime an authenticated user initiates remote access, file transfer or software distribution. These logs are archived for up to 7 years in order to meet customer audit requests, should a breach or unauthorized access be suspected.

Through RSS Customer Portal, customers can additionally audit remote access to BD Products.

Remote Connectivity

BD Remote Support Services (RSS) is BD's remote connectivity solution.

Service Handling

BD employees who use the RSS dashboard are trained in the HIPAA, HITECH and U.S. Federal regulations relevant to supporting BD products. Sensitive data handling training (ePHI, HIPAA, or E.U. Data Privacy) for RSS users that are non-BD employees or outside of the U.S. is addressed separately, per individual contract.

DOD: BD employees must get Government Security Clearance before being approved by BD for access to DOD devices.

End-of-Life and End-of-Support

There is currently no end-of-life or end-of-support for the RSS platform.

Secure Coding Standards

Fortify on Demand (FOD) is being used for adherence to secure coding standards.

System Hardening Standards

- FDA Cybersecurity Guidelines
- NIST SP 800-53 Rev. 4
- DISA STIG
- HIPAA Privacy & Security Rules
- NSA Guides
- OWASP Top 10

BD Supported Products

BD Medication and Procedural Solutions	BD Biosciences	BD Diagnostic Systems
BD Pyxis™ ES System **	BD FACSAria™ II	BD EpiCenter™
BD Pyxis™ MedStation™ 4000 System **	BD FACSAria™ III	BD MAX™
BD Pyxis™ MedStation™ 3500 System **	BD FACSAria™ Fusion	BD Viper™ LT
BD Pyxis™ MedStation™ 3000 System	BD FACSCanto™ A	BD BACTEC™ FX, FX40
BD Pyxis™ Logistics **	BD FACSCanto™ II	BD Viper™ XTR
BD Pyxis™ Check	BD FACSCanto™ 10-color	BD Synapsys™
BD Pyxis™ Order Viewer	BD FACSCelesta™	BD Phoenix™ M50
BD Pyxis™ IV Prep (US Only) ** BD Cato™ (EU Only)	BD FACSLink™	
BD Pyxis™ CIISafe **	BD LSRFortessa™ II	

BD Medication and Procedural Solutions	BD Biosciences	BD Diagnostic Systems
BD Pyxis™ SupplyStation™ **	BD LSRFortessa™	
BD Pyxis™ SupplyCenter **	BD LSRFortessa™ X-20	
BD Pyxis™ SupplyCenter VM **	BD FACSymphony™	
BD Alaris™ System Manager Server **		
Pyxis™ PARx™		
BD Care Coordination Engine (CCE) **		
Security Module **		
MedMined™ services		

** Leverage windows patch management functionality within RSS.

Risk Summary

A vulnerability scan was performed on the instrument under operation. The following vulnerabilities were revealed and should be considered for installation planning and operational procedures:

- Multi-factor authentication is not currently supported
  Exception: customer initiated remote support sessions do not require multi-factor authentication
- Application log file retention is not standardized across the RSS platform and varies due to disk space constraints

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 effectives of controls to meet the applicable criteria.

As part of this year's fourth annual 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

Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category Not Applicable	Manufacturer CareFusion	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model BD Remote Support Services (RSS)	Software Revision [version]	Software Release Date [YYYY-MM-DD]	

Manufacturer or Representative Contact Information	Company Name BD (Becton, Dickinson, and Company)	Manufacturer Contact Information Becton, Dickinson and Company Attn: Product Security and Privacy 1 Becton Drive, Franklin Lakes, New Jersey 07417-1880
	Representative Name/Position [Customer support number]	

Intended use of device in network-connected environment:

Not Applicable

Intended purpose of integrating the Device into an IT-Network:
[e.g. Remote Service, EMR, LIS, HIS]

MANAGEMENT OF PRIVATE DATA

Device Category Not Applicable	Manufacturer CareFusion	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model BD Remote Support Services (RSS)	Software Revision [version]	Software Release Date [YYYY-MM-DD]	

	Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [**ePHI**])?	_YES_____	__
B	Types of **private data** elements that can be maintained by the **device**:		
	B.1 Demographic (e.g., name, address, location, unique identification number)?	_YES_____	__
	B.2 Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	_Yes_____	__
	B.3 Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	_NO_____	__
	B.4 Open, unstructured text entered by **device user/operator**?	_NO_____	__
	B.5 **Biometric data**?	_NO_____	__
	B.6 Personal financial information?	_NO_____	__
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?	_NA_____	__
	C.3 Import/export **private data** with other systems?	_NA_____	__
	C.4 Maintain **private data** during power service interruptions?	_NA_____	__
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:	_NA_____	
	D.1 Display **private data** (e.g., video display, etc.)?	_NA_____	__
	D.2 Generate hardcopy reports or images containing private data?	_NA_____	__

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.)?	_NA_____	__
D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	_NA_____	__
D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	_YES_____	__
D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	_NA_____	__
D.7	Import **private data** via scanning?	_NA_____	__
D.8	Other?	_NA_____	__

Management of **private data** notes:

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.	Yes, No, N/A, or See Note	Note #

1 AUTOMATIC LOGOFF (ALOF)
The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.

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)?	__Yes__	__
1-1.1	Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	yes	__
1-1.2	Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	__Yes__	__

ALOF notes: [The hint to the “Security Package” is not enough. Please write more details about the behavior of the system.]

Device Category	Manufacturer	Document ID	Document Release Date
Not Applicable	CareFusion	[e.g. 234-234323]	[YYYY-MM]
Device Model	**Software Revision**	**Software Release Date**	
BD Remote Support Services (RSS)	[version]	[YYYY-MM-DD]	

2 AUDIT CONTROLS (AUDT)
The ability to reliably audit activity on the **device**.

2-1	Can the **medical device** create an **audit trail**?	Yes	__
2-2	Indicate which of the following events are recorded in the audit log:		
2-2.1	Login/logout	__Yes__	__
2-2.2	Display/presentation of data	__NA__	__
2-2.3	Creation/modification/deletion of data	__NA__	__
2-2.4	Import/export of data from **removable media**	__NA__	__
2-2.5	Receipt/transmission of data from/to external (e.g., network) connection	__NA__	__
2-2.5.1	**Remote service** activity	__NAYes __	__

	2-2.6 Other events? (describe in the notes section)	__NA__	__
2-3	Indicate what information is used to identify individual events recorded in the audit log:		
	2-3.1 **User** ID	__Yes__	__
	2-3.2 Date/time	__Yes__	__
AUDT notes:	[The hint to the “Security Package” is not enough. Please write more details about the behavior of the system.]		

3	**AUTHORIZATION (AUTH)** The ability of the **device** to determine the authorization of **users**.		
3-1	Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?	__Yes_ _	__
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	__Yes_ _	__
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	__No__	__
AUTH notes:	[The hint to the “Security Package” is not enough. Please write more details about the behavior of the system.]		

Refer to Section 2.3. of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
4 **CONFIGURATION OF SECURITY FEATURES (CNFS)** The ability to configure/re-configure **device security capabilities** to meet **users’** needs.		
4-1 Can the **device** owner/**operator** reconfigure product **security capabilities**?	_Yes__	__
CNFS notes:		

5	**CYBER SECURITY PRODUCT UPGRADES (CSUP)** The ability of on-site service staff, **remote service** staff, or authorized customer staff to install/upgrade **device**'s security patches.		
5-1	Can relevant OS and **device** security patches be applied to the **device** as they become available?	__Yes__	__
	5-1.1 Can security patches or other software be installed remotely?	_Yes__	__
CSUP notes:	[Please let it also know **who** is authorize to install security patches]		

6	**HEALTH DATA DE-IDENTIFICATION (DIDT)** 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**?	__Yes__	__
DIDT notes:	[Details to the anonymization function are recommended]		

Device Category Not Applicable	Manufacturer CareFusion	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model BD Remote Support Services (RSS)	Software Revision [version]	Software Release Date [YYYY-MM-DD]	

7	**DATA BACKUP AND DISASTER RECOVERY (DTBK)** 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)?	__Yes__	__
DTBK notes:	[Information to the applicable procedure are necessary]		
8	**EMERGENCY ACCESS (EMRG)** 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** ("break-glass") feature?	__NA__	__
EMRG notes:	[If there are restrictions additional informations are required.]		
9	**HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)** 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?	__Yes__	__
IGAU notes:			

Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.		Yes, No, N/A, or See Note	Note #
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)?	__NA__	__
10-1.1	Can the **user** independently re-configure **anti-malware** settings?	__NA__	__
10-1.2	Does notification of **malware** detection occur in the **device user** interface?	__NA__	__
10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected? ..	__NA__	__
10-2	Can the **device** owner install or update **anti-virus software**?	__NA__	__
10-3	Can the **device** owner/**operator** (technically/physically) update **virus** definitions on manufacturer-installed **anti-virus software**?	__NA__	__
MLDP notes:	[Information about the time schedule is needed. As appropriate refer to service contract and/or SLA.]		
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?	__NA__	__
NAUT notes:	[Please consider remote access too]		
12	**PERSON AUTHENTICATION (PAUT)** Ability of the **device** to authenticate **user**s		
12-1	Does the **device** support **user**/**operator**-specific username(s) and password(s) for at least one **user**?	__NA__	__
12-1.1	Does the **device** support unique **user**/**operator**-specific IDs and passwords for multiple **users**?	__NA__	__
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	__Yes__	__
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	__NA__	__
12-4	Can default passwords be changed at/prior to installation?	__NA__	__

12-5	Are any shared **user** IDs used in this system?	__No__	__
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	__NA__	__
12-7	Can the **device** be configured so that account passwords expire periodically?	__NA__	__

PAUT notes: [If 12-2 Yes, then additional information to the applicable methods are important. Especially for MS Active Directory.]

Device Category Not Applicable	Manufacturer CareFusion	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model BD Remote Support Services (RSS)	Software Revision [version]	Software Release Date [YYYY-MM-DD]	

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)?	__NA__	__

PLOK notes:

Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

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).	__NA__	__
14-2	Is a list of other third party applications provided by the manufacturer available?	__NA__	__

RDMP notes:

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__	__
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.)?	__NA__	__
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)?	__NA__	__
15-5	Are all accounts which are not required for the **intended use** of the **device** disabled or deleted, for both users and applications?	__NA__	__
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	__NA__	__
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	__NA__	__

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?	__NA__	__
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?	__NA__	__
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	__NA__	__
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	__NA__	__

SAHD notes: [Mentioned 15-7: A list of the opened ports are strongly recommended]

Device Category	Manufacturer	Document ID	Document Release Date
Not Applicable	CareFusion	[e.g. 234-234323]	[YYYY-MM]
Device Model	**Software Revision**	**Software Release Date**	
BD Remote Support Services (RSS)	[version]	[YYYY-MM-DD]	

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**?	__NA__	__
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)?	__NA__	__

SGUD notes:

Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
17 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**.		
17-1 Can the **device** encrypt data at rest?	__Yes_ _	__
STCF notes: [IfYes, additional information about the method is recommended]		
18 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?	__Yes__	__
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.)	__Yes__	__
18-3 Is **private data** transmission restricted to a fixed list of network destinations?	__Yes__	__
TXCF notes:		
19 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? (If yes, describe in the notes section how this is achieved.)	__NA_	
TXIG notes:			

20	**OTHER SECURITY CONSIDERATIONS (OTHR)** Additional security considerations/notes regarding **medical device** security.		
20-1	Can the **device** be serviced remotely?	__Yes_	
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	__Yes_	
20-2.1	Can the **device** be configured to require the local **user** to accept or initiate remote access?	__Yes_	
OTHR notes:			

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.