Product Security White Paper

Arctic Sun™ Analytics

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 (GDPR) (EU) 2016/679.

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™ Analytics, 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

Arctic Sun Analytics is a web-based application that provides clinicians and administrators retrospective analytics on clinical and process variability related to Targeted Temperature Management (TTM) using the Arctic Sun device. (Note: Please refer to Arctic Sun Whitepaper for further device specific security information.) This information can then be used, in combination with hospital care protocols and patient information, to help drive process improvement which leads to improved patient care.

Hardware Specifications

Client: Users leverage a standard web browser to access the applications. The computer used to run the browser is provided by the customer.

- Arctic Sun Analytics client can run on the following browsers:
  - Microsoft^{TM} Internet Explorer^{TM} 11 (latest)
  - Google^{TM} Chrome^{TM} (latest)

Server: The applications are hosted on Microsoft Azure Platform as a Services (PaaS).

Operating Systems

Client: Users leverage a standard web browser to access the applications. The operating system used is at the customer's discretion.

Server: The applications are hosted on Microsoft Azure Platform as a Services (PaaS).

Third-party Software

Client:

- PDF Viewer - Provided by customer

Server:

Programming Languages

- C#
- JavaScript
- TypeScript

Libraries and Frameworks

- ASP.NET Core
- Prime NG
- D3JS
- Bootstrap
- RXJS

Databases, Web Services, Cloud Services

- Microsoft Azure App Service
- Microsoft Azure Functions
- Microsoft Azure SQL Server

- Microsoft Azure Event Hub
- Microsoft Azure Stream Analytics
- Microsoft Azure Storage
- Microsoft Azure Redis Cache

Operations

- Microsoft Application Insights
- Terraform
- Octopus

Network Ports and Services

All communications between the hospital and the application are via port 443.

Port	Protocol	Service Name	Description of Service	Encrypted	Open/Closed
443	HTTPS	Azure App Service • www.carefusionanalytics.com • cloud.bd.com • ASA.BD.com	Web Application accessible to users	YES	Open

Sensitive Data Transmitted

- Patient First Name
- Patient Last Name
- Medical Record Number (MRN)
- Patient Gender
- Patient DOB
- Patient Weight
- Patient Height
- Admit Date
- Admit Time
- Patient Outcome
- Return of spontaneous circulation (ROSC) Date
- ROSC Time

All sensitive data transmitted is encrypted. See the encryption section below for more information.

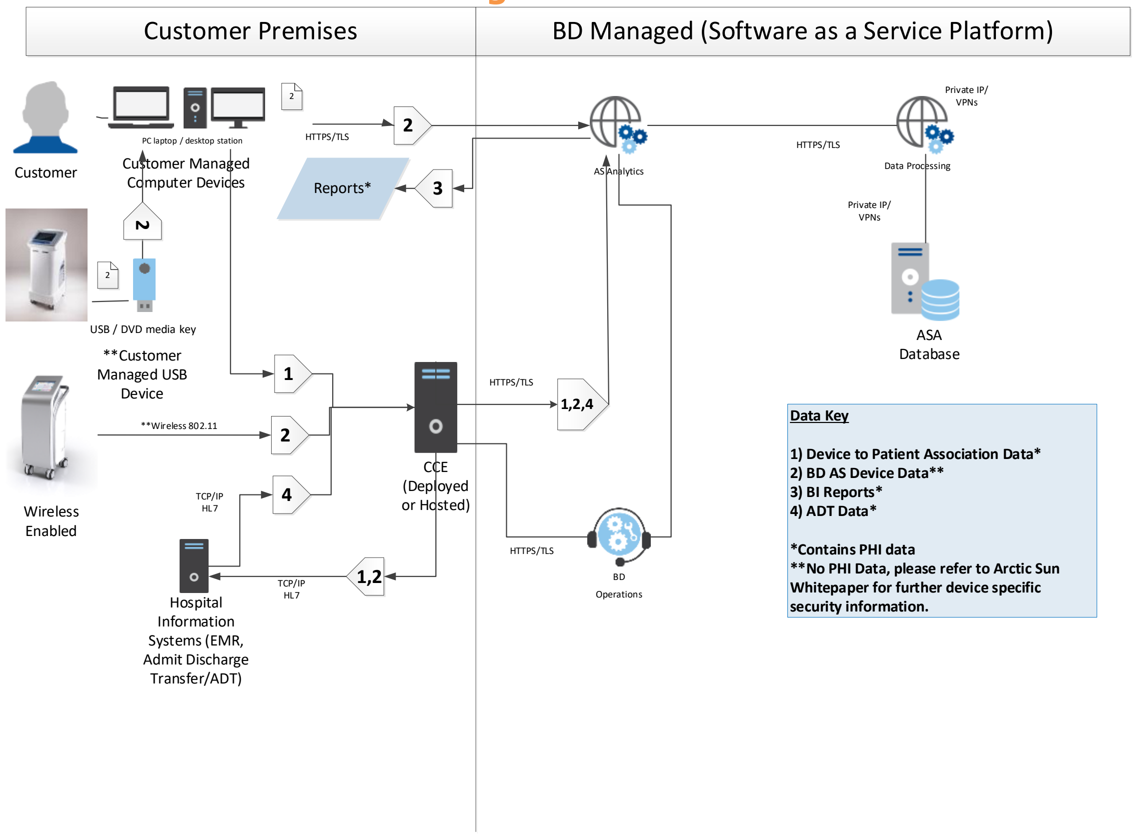
Sensitive Data Stored

- Patient First Name
- Patient Last Name
- Medical Record Number (MRN)
- Patient Gender
- Patient DOB
- Patient Weight

- Patient Height
- Admit Date
- Admit Time
- Patient Outcome
- ROSC Date
- ROSC Time

All sensitive data stored is encrypted. See the encryption section below for more information.

Network and Data Flow Diagram



Data Key

1) Device to Patient Association Data*
2) BD AS Device Data**
3) BI Reports*
4) ADT Data*

***Contains PHI data**
****No PHI Data, please refer to Arctic Sun Whitepaper for further device specific security information.**

Note: Please refer to Arctic Sun Whitepaper for further device specific security information.

Malware Protection

Azure Cloud Platform as a Service Solution, PaaS Assets are managed by Microsoft. See Microsoft article for more information: https://docs.microsoft.com/en-us/azure/security/fundamentals/paas-deployments

Patch Management

BD proactively monitors and manages patching for the applications' hosted environment according to BD policy.

- Medium to Critical Risks: Patches must be applied within 30 days after initial discovery.
- Low Risks: May be addressed separately in a reasonable amount of time however, at a minimum, during the next product or software update.

Note: Azure Cloud Platform as a Service Solution, PaaS Assets are managed by Microsoft. See Microsoft article for more information: https://docs.microsoft.com/en-us/azure/app-service/overview-patch-os-runtime

Authentication Authorization

Arctic Sun Analytics customers authenticate against a BD managed identity management system.

In the BD-provided identity management system, sensitive data is stored using AES256 encryption. Authorization is managed in the BD application. No customer roles have full system admin rights.

BD's hosted applications authenticate BD employees against a Microsoft® Active Directory instance that is maintained by BD. Once a new employee has been granted an account, his/her direct management must provide additional training, including electronic PHI (ePHI) handling and authorization, before they receive access to the Arctic Sun Analytics application. In the event that an employee leaves, BD suspends their account as a part of its standard off-boarding procedures. BD maintains an audit log of all users who have been granted access, both employees and customer users.

BD support personnel authenticate via a BD-maintained Microsoft Active Directory instance.

Network Controls

Client: The application is accessed from a customer provided environment. In order to access the application, the client network must allow communication to the BD Hosted Environment. See Network Ports and Services section for ports and protocols to be open for application communication. Recommended browser is latest version of Chrome.

Server: All network access is controlled and monitored by BD Operations team. Access to production infrastructure is limited to supporting personnel via role-based controls.

Encryption

Web application traffic is transmitted via TLS 1.2. The database, Azure SQL Database, has Transparent Data Encryption enabled.

See Microsoft article for more information: https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?tabs=azure-portal

Audit Logging

Audit logs are stored in Microsoft Application Insight and is kept for 730 days. The Arctic Sun™ Analytics application logs the following system information:

- Date Accessed
- Time Accessed
- User identification
- Action parameters for any activity that accesses or modifies data. Actions include:
    - User Login
    - User Logoff
    - Files/Records Modified
    - Files/Records Deleted
    - Failed login attempts

See Microsoft article for more information: https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy#how-long-is-the-data-kept

Using temporal tables to capture full history of changes in database. Database data is stored for 3 years and then moved into long term storage.

Remote Connectivity

Remote connectivity to BD's Azure subscription is allowed for certified support personnel via Azure Portal.

Service Handling

Service handling is performed by BD Operations. BD has an access management process in place to request, approve, and review access to production environments. BD employees must take electronic PHI (ePHI) handling and authorization training as a pre-requisite to gaining access. In the event an employee leaves BD or transfers to a different position, BD removes their access. BD maintains an audit log of all users (customer and employee). Please see the Patch Management, Network Controls, and Authentication and Authorization sections for further information on those topics.

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

Fortify on Demand is used as the static code analysis tool for these applications. The following secure coding standards are adhered to during development of these applications:

- Microsoft best practices
- OWASP Top 10 threats

System Hardening Standards

The following standards and guidelines are used in the software development and operational procedures used to support the production environments:

- FDA Cybersecurity Guidelines
- HIPAA Privacy & Security Rules
- NSA Guides
- OWASP Top 10
- NIST 800-66

Risk Summary

A security assessment was performed on the Azure Hosted environment under operation. The following vulnerabilities were revealed and should be considered for installation planning and operational procedures:

- BD hosted applications are accessed by customers through browser technology.
    - Security of the system relies on the customer to properly manage the security settings of the browser as well as the underlying operating system by ensuring secure best practices such as antivirus are employed.

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 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

Arctic Sun™ Analytics is not a regulated medical device nor is it software that runs on a medical device. As a result, this section has been left empty.

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.