GENERAL INSTRUCTIONS

This Product Security White Paper Template is utilized to enable transparency and coordination with customers for robust medical device security partnership. The template provides an outline of the type of information to be included and is to be filled out by each product team. All items in red text should be replaced with the appropriate response.

Product Security White Paper

[insert company's stance regarding product security].

[insert company's name] has implemented reasonable administrative, technical and physical safeguards to help protect against security incidents and privacy breaches involving a [insert company's name] product, provided those products are used in accordance with [insert company's name] 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. [insert company's name] 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 [insert company's name]

If you would like to report a potential product related privacy or security issue (incident, breach or vulnerability), please contact [insert company's contact information here].

The purpose of this document is to detail how [insert company's name] security and privacy practices have been applied to the [Insert Product Name], 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

[Insert basic description of function or purpose of the product or solution. Photo is optional, but recommended.]

Hardware Specifications

[List Hardware Components and Specs]

- List
- List
- List

Operating Systems

[List Hardware Operating Systems and Versions]

- List
- List
- List

Third-party Software

[List Third-Party Software]

Vendor and Name	Version	Description
XXXXX	XXX	XXXXX

Network Ports and Services

[List Network Ports and Services]

Port	Protocol	Service Name	Description of Service	Encrypted	Open/Closed
XXX	XXX	XXXXX	XXXXX	XXX	XXX

Sensitive Data Transmitted

[List Sensitive Data Transmitted. This can include PHI/PII/Potential access to wireless credentials, etc.]

- List
- List

Sensitive Data Stored

[List Sensitive Data Stored. This can include PHI/PII/Potential access to wireless credentials, etc.]

- List
- List

Network and Data Flow Diagram

[Provide a diagram that describes how the product resides in a customer environment, showing the system components (1 or N computers, routers, switches, adjacent systems, remote connectivity) types of connectivity (e.g. RS232, RJ45, Serial to TCP/IP conversion), what types of data is in transit and at rest (e.g. PHI, QC, config data), and how these are secured (e.g. in transit IPSec, HTTPS/TLS, WIFI WPA2PSK; at rest BitLocker, SQL TDE)]

Malware Protection

[Describe and recommend the antimalware measures available (e.g. validated AV solutions, AV partners, how AV is managed, Application Whitelisting like AppLocker or McAfee Embedded Control, advanced antimalware solutions, Software Restriction Policies)]

Authentication Authorization

[Describe and recommend the controls that customers have with user's authenticating and granting permissions to features and functionality, how users are managed, the default use accounts on the system and how to change and configure accounts]

Network Controls

[Describe and recommend the firewall rules, IPSec rules, host file restrictions, browser Internet access restrictions, MAC and IP address filtering)]

Encryption

[Describe and recommend where and how encryption is applied on the system (e.g. all network traffic is TLS 1.2, at rest is BitLocker with AES 256)]

Audit Logging

[Describe the audit logging process, where they are stored, what an auditable event entails, who has access to audit logs and any file permissions].

- i.e. Application Auditing
  - Audit file location: E:\PieRoot\Logfiles\*.pld
  - Audit files hashed with SHA256 when complete for integrity.
  - Auditable Events:
    - Service Start/Stop
    - User login/logout
    - User session created/destroyed.
    - User login from multiple workstations.
    - Client application connect/disconnect with IP address and port.
    - Failed client connection attempts.
    - Changes in application configuration.
    - Failed/successful attempts to access, modify, or delete security objects; e.g. roles, permissions, etc.

- Audit file permissions:
    - Administrators group: Read.
    - Auditors group: Read.
    - DB Auditors group: Full control.
    - DB Administrators group: Full control.
    - Virtual/Managed service accounts (audit file creators): Full control.
    - Users: None.

Remote Connectivity

[Describe the nature of remote connectivity, what ports, protocols, URLs and endpoints for communication as well as security measures applied to the remote connection (e.g. TLS,)]

Service Handling

[Describe what routine maintenance service personal perform, what security policies and procedures they follow (e.g. never take PHI or PII, on-site authorization protocol, encrypted removable media, hardened service laptops, whether or not service laptops connect to product, routine AV update during visit, secure installation/implementation principles, service authentication to product, decommissioning process, once decommissioned how the product hard drive is wiped, how the product is recovered from the field or destroyed, and what customer data and features service personnel interact with)]

End-of-Life and End-of-Support

[Describe the life cycle of the product in relation to when it will no longer be sold, updated, and supported. Provide dates if available, otherwise describe how EOL/EOS is communicated.]

Secure Coding Standards

[Describe the secure coding standards used]

- [List the industry secure coding standards used during software development (e.g. SEI CERT Java Secure Coding Standard)]

System Hardening Standards

[Describe the secure hardening standards used, may also create appendix to list out standards used.]

Name of Standard	Version Number	Source of Standard
[Insert name of standard]	[Insert version number]	[Insert URL]

Risk Summary

[This section should contain a summarization of risks found within a penetration test, remediation report, or other topics and compensating controls that correspond to additional risks outlined in the product security white paper. This may also include any findings from application scans.]

Third Party Soc2+ Reporting

[Delete this section if a SOC2 audit is not available for your product.
Check with your Product Security group to determine if you product is within scope.]

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

[Intentionally left blank]

Manufacturer's Disclosure Statement for Medical Device Security

Otherwise known as the MDS2 form, this section provides an industry standard convention for security information. [Use section even if not a "regulated" medical device. Delete spaces in-between tables and ensure the first two rows of the Device Description category are displayed on every page.]

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

DEVICE DESCRIPTION

Device Category [enter text and code here]	Manufacturer [insert company's name]	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model [product name]	Software Revision [version]	Software Release Date [YYYY-MM-DD]	

Manufacturer or Representative Contact Information	Company Name [insert company's name]	Manufacturer Contact Information [insert company contact information]
	Representative Name/Position [Customer support number]	

Intended use of device in network-connected environment:

[enter the Intended use here as stated in 510(k) clearance or PMA approval.]

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

[e.g. Remote Service, EMR, LIS, HIS]

MANAGEMENT OF PRIVATE DATA

		Yes, No, N/A, or See Note	Note #
	Refer to Section 2.3.2 of HIMSS/NEMA HN 1-2013 standard for the proper interpretation of information requested in this form.		
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [**ePHI**])?	______	__
B	Types of **private data** elements that can be maintained by the **device**:		
B.1	Demographic (e.g., name, address, location, unique identification number)?..................................	______	__
B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	______	__

B.3 Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)? .... ______ __

B.4 Open, unstructured text entered by **device user**/**operator**? .... ______ __

B.5 **Biometric data**? .... ______ __

B.6 Personal financial information? .... ______ __

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)? ...... ______ __

C.2 Store **private data** persistently on local media? .... ______ __

C.3 Import/export **private data** with other systems?........ ______ __

C.4 Maintain **private data** during power service interruptions? .... ______ __

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

D.1 Display **private data** (e.g., video display, etc.)? .... ______ __

D.2 Generate hardcopy reports or images containing private data? .... ______ __

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.)? .... ______ __

D.4 Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)? .... ______ __

D.5 Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)? .... ______ __

D.6 Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)? .... ______ __

D.7 Import **private data** via scanning? .... ______ __

D.8 Other? .... ______ __

Management of **private data** notes: [Fill in]

Device Category [enter text and code here]	Manufacturer [insert company's name]	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model [product name]	Software Revision [version]	Software Release Date [YYYY-MM-DD]	

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)? .... ______ __

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.) .... ______ __

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

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

2 AUDIT CONTROLS (AUDT)

The ability to reliably audit activity on the **device**.

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) .... ______ __

2-3 Indicate what information is used to identify individual events recorded in the audit log:

2-3.1 **User** ID .... ______ __

2-3.2 Date/time .... ______ __

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? ______ __

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

Device Category [enter text and code here]	Manufacturer [insert company’s name]	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model [product name]	Software Revision [version]	Software Release Date [YYYY-MM-DD]	

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**? .... ______ __

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? .... ______ __

5-1.1 Can security patches or other software be installed remotely? .... ______ __

CSUP notes: [Please let it also know **who** is authorized 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**? .... ______ __

DIDT notes: [Details to the anonymization function are recommended]

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)? .... ______ __

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? .... _____ __

EMRG notes: [If there are restrictions additional information’s 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? .... ______ __

IGAU notes:

Device Category [enter text and code here]	Manufacturer [insert company's name]	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model [product name]	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 #

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)? .... ______ __

10-1.1 Can the **user** independently re-configure **anti-malware** settings? .... ______ __

10-1.2 Does notification of **malware** detection occur in the **device user** interface? .... ______ __

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

10-2 Can the **device** owner install or update **anti-virus software**? .... ______ __

10-3 Can the **device** owner/**operator** (technically/physically) update **virus** definitions on manufacturer-installed **anti-virus software**? .... ______ __

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? .... ______ __

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**? ..... ______ __

12-1.1 Does the **device** support unique **user**/**operator**-specific IDs and passwords for multiple **users**? .... ______ __

12-2 Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)? .... ______ __

12-3 Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts? . ______ __

12-4 Can default passwords be changed at/prior to installation? .... ______ __

12-5 Are any shared **user** IDs used in this system? .... ______ __

12-6 Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules? .... ______ __

12-7 Can the **device** be configured so that account passwords expire periodically? .... ______ __

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

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)? .... ______ __

PLOK notes:

Device Category [enter text and code here]	Manufacturer [insert company's name]	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model [product name]	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 #

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? ______ __

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. ______ __

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? ______ __

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

______ __

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)?

______ __

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

______ __

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

______ __

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

______ __

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?

______ __

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?

______ __

15-10 Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?

______ __

15-11 Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?

______ __

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

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**?

______ __

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)?

______ __

SGUD notes:

Device Category [enter text and code here]	Manufacturer [insert company's name]	Document ID [e.g. 234-234323]	Document Release Date [YYYY-MM]
Device Model [product name]	Software Revision [version]	Software Release Date [YYYY-MM-DD]	

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

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? ______ __

STCF notes: [If Yes, 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? ______ __

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.) ______ __

18-3 Is **private data** transmission restricted to a fixed list of network destinations? ______ __

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.) ______ __

TXIG notes:

20 OTHER SECURITY CONSIDERATIONS (OTHR)

Additional security considerations/notes regarding **medical device** security.

20-1 Can the **device** be serviced remotely? ______ __

20-2 Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)? ______ __

20-2.1 Can the **device** be configured to require the local **user** to accept or initiate remote access? .... ______ __

OTHER
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 [insert company's name], or [insert company's name] subsidiaries or affiliates (collectively, "[insert company's name]"). [insert company's name] 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.