Providence

Enterprise Information Security
Vendor Security Assessment

*** * * To be completed by the Vendor representative * * ***

Important Instructions

- All questions in this assessment are mandatory. Answer all questions to the best of your knowledge and ability. Incomplete or inaccurate assessment forms will not be reviewed and may result in processing delays, an unfavorable rating, and/or the exclusion of the vendor solution from Providence's environment or use with Providence data.
- The vendor representative who is completing this form must have sufficient knowledge of the system or service to accurately and completely represent their product.
- Not all sections will apply. If a section is not mandatory and does not apply, mark the checkbox indicating that the section does not apply, and proceed to the next section as instructed in the form.
- All 'N/A' and 'No' responses require an explanation in the corresponding *Vendor Comments* field. 'N/A' and 'No' responses that do not have a corresponding rationale in the comments field will not be accepted and may result in a finding.
- Comments are encouraged for 'Yes' answers as well, because this information can help provide additional context to the reviewer. If your organization has strong security controls, please use the Vendor Comments section to highlight those controls even for 'Yes' answers. However, additional comments corresponding to 'Yes' answers are not required unless otherwise specified.
- NOTE: Some fields require an entry into the corresponding *Vendor Comments* field regardless of the answer. Questions of this nature usually have a secondary question or information request in a parenthetical statement below the primary question.
- DO NOT alter the content of this document. Provide your answers only in the space allocated to do so. Any unauthorized document changes that are detected may result in processing delays, an unfavorable rating, and/or the exclusion of the Vendor's solution from Providence's environment or use with Providence data.
- DO NOT convert this questionnaire to a PDF or other document format because Providence security analysts will use this form to complete their assessment and file the results.
- For systems or services that store, process, or transmit Payment Card Information (PCI), transactions or storage involving credit or debit card information, please return the documents requested below along with this completed form.

Security Review Status Definitions

Satisfactory – Vendor responses to the Vendor Security Assessment (VSA) questionnaire demonstrated that the system or service exhibited no material findings and is capable of meeting Providence requirements (i.e., policies, standards, regulatory requirements, contractual and legal obligations, and relevant federal, state, and local laws). While the Vendor system or service has been determined to be capable of meeting Providence requirements, stakeholders are nonetheless responsible to ensure that the system or service is configured, deployed, and operationalized in accordance with such requirements. Default or Vendor-recommended configurations, deployment methods, and operating practices may not be consistent with Providence requirements. Questions about whether a configuration, deployment method, or operating practice is in accordance with Providence requirements can be directed to the analyst who conducted the VSA or to the Information Security Risk Advisory general mailbox: InfoSecRiskAdvisory@providence.org. In addition to the VSA, further EIS follow-up reviews (e.g., Security Engineering and Security Architecture reviews, etc.) may be required prior to deployment, depending on the criticality, complexity, and risks associated with the system or service. Systems and services that were assigned a Satisfactory rating generally represent Very Low or Low risk to Providence, if configured, deployed, and operated in accordance with Providence requirements.

Satisfactory with Conditions – Vendor responses to the Vendor Security Assessment (VSA) questionnaire demonstrated that the system or service exhibited material findings and was partially incapable of meeting Providence security requirements (i.e., policies, standards, regulatory requirements, contractual and legal obligations, and relevant federal, state, and local laws). Use of the system or service could adversely impact the confidentiality, integrity, and availability of Providence systems or data. Enterprise Information Security (EIS) will communicate specific VSA findings and their associated risks to the Providence business, technology, or data owner. If the business, technology, or data owner chooses to proceed with the deployment or use of the Vendor's system or service, despite his or her awareness of the findings and associated risks, he or she is fully responsible for the risks and the adverse impact that such risks could have on Providence. Likewise, the business or data owner is responsible for working directly with the Vendor to remediate the security control gaps that have generated the risks. In some cases (to be determined by EIS on a case-by-case basis), EIS may require the business, technology, or data owner to formally accept the risks, and the risks will be tracked in the Providence Risk Register system until they are adequately mitigated. Members of EIS will, in most circumstances, be available to provide guidance and security risk consultation as the business, technology, or data owner works to remediate the findings and associated risks. In most cases, business, technology, or data owners, or their designees, should work with the analyst who conducted the VSA. However, they can also direct inquires to the Information Security Risk Advisory general mailbox: InfoSecRiskAdvisory@providence.org. Systems and services that were assigned a Satisfactory with Conditions rating generally represent a Moderate risk to Providence, if configured, deployed, and operated in a manner that is consistent, to the extent that they are capable, with Providence requirements.

Fail – Vendor responses to the Vendor Security Assessment (VSA) questionnaire demonstrated that the system or service exhibited significant security gaps and/or regulatory non-compliance. A clear and timely path to risk mitigation is not currently possible. Use of this application or service represents a significant risk to Providence systems, data, and possibly patient safety. The system or service is **not** approved for Providence use. Systems or services that were assigned a Fail rating represent a High or Very High risk to Providence.

Acronyms and Terms:

AD: Active Directory

AES: Advance Encryption Standard

BAA: Business Associate Agreement

EIS: Enterprise Information Security (Providence's Information Security department)

IaaS: Infrastructure as a Service

LDAP: Lightweight Directory Access Protocol

LEEF: Log Event Extended Format

OS: Operating System

PCI: Payment Card Industry (See expanded definition under Confidential Data Types below)

PHI: Protected Health Information (See expanded definition under Confidential Data Types below)

PII: Personally Identifiable Information (See expanded definition under Confidential Data Types below)

Providence: Providence Saint Joseph Health

PaaS: Platform as a Service

SaaS: Software as a Service

SIEM: Security Information and Event Management

SSAE 16 or 18 SOC II: Statement on Standards for Attestation Engagements (report on compliance controls)

SSL: Secure Socket Layer

SSO: Single Sign-On

Subcontractor: Any individual, corporation, partnership, joint venture, limited liability company, or other such entity that is, at any time during the term of an agreement with Providence, performing work on behalf of the Primary Vendor (meaning the company or organization completing this assessment questionnaire.)

Vendor or Primary Vendor: For the purposes of this assessment, a Vendor is a HIPAA Business Associate, HIPAA Covered Entity, technology or services vendor, or any other non-Providence business partner performing a technical or business function, either through a contract or other formal agreement, for Providence. The term Vendor does not include software resellers or consultants implementing a solution.

VPN: Virtual Private Network

Confidential Data Types Defined:

Personally Identifiable Information (PII): PII is any piece of information that could potentially be used to identify, contact, or locate an individual. This includes, but is not limited to:

- Social Security Number
- Driver's license or state identification card number
- Date of birth
- Financial information, such as credit or debit card numbers
- Password or PIN number
- Address information, such as street address or email address
- Telephone numbers, including mobile, business, and personal numbers

Protected Health Information (PHI) / electronic Personal Health Information (ePHI): Any information, including demographic information, that is created or received by a HIPAA Covered Entity (e.g., healthcare institution, health insurance provider) or a Business Associate (e.g., a vendor or service provider used by a Covered Entity) and relates to:

- the past, present, or future physical or mental health or condition of an individual;
- the provision of health care to an individual;
- the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information concerning persons living or deceased (less than 50 years) and may be written, oral or electronic.

There are 18 identifiers that constitute PHI.

1. Names
2. All geographic subdivisions smaller than a state, including: street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial 3 digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic unites containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/License numbers
12. Vehicle Identifiers and serial numbers (including license plates)
13. Device identifiers and serial numbers
14. URL addresses
15. IP addresses
16. Biometric identifiers, including fingerprints and voiceprints
17. Full face photos and any comparable images
18. Any other unique identifying number, characteristic or code

Confidential Information (Business Confidential Information or Intellectual Property): Any information, regardless of format, about patients, workforce members, or business operations that:

- an organization is legally required to keep confidential;
- an organization deems should not be available without specific authorization; or
- a workforce member should reasonably understand to be proprietary to an organization or otherwise should be maintained confidentially.

Loss or inappropriate access to Confidential Information may cause harm to the privacy of patients or harm to an organization's ability to conduct business. Confidential information includes but is not limited to PHI, ePHI, PII including SSNs, payment card holder data (PCI), financial information, intellectual property, and research data. Other examples of confidential information include but are not limited to chemical dependency or mental health information, employee/personnel records, privileged information from internal/external counsel, board, board committee (at any level of the organization) or medical staff committee minutes, notes or actions, non-public financial, strategic or operational information, trade-secrets or other confidential information or processes used by an organization in carrying out its activities, and information which an organization or one of its business lines has agreed to keep confidential.

Payment Card Industry (PCI): The PCI Standards Council is a consortium of card brands (e.g., Visa, MasterCard, and Amex) and sponsoring companies that establish standards for card-processing functions. PCI information is any cardholder data elements which, at a minimum, includes data that comprises the full Primary Account Number (PAN), credit or debit card number. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.

* * * Start Questionnaire * * *

Vendor Contact Information [Required – Do not skip]

Date: 16 Sep 2022	16 Sep 2022
Vendor Contact Name: Cody Gamble	Product or Service Name(s): Avvigo II
Vendor Contact Title: Business Partner	Vendor Website: www.bostonscientific.com
Vendor Contact Email: cody.gamble@bsci.com	Vendor Support Phone Number: 1-509-939-9047
Vendor Contact Phone Number: 1-509-939-9047	Name of Primary Providence Stakeholder: Ashley Davis/Saint Patricks

Vendor Security Contact Information	
Security Contact Name: Product CyberSecurity	Security Contact Phone Number: Click here to enter text.
Security Contact Title: Click here to enter text.	Security Contact Email: productcybersecurity@bsci.com

General Information [Required – Do not skip]

Complete all fields below. If you are uncertain about how to answer a question, please contact the assigned security analyst or the Providence point of contact.

Provide a brief summary of the Vendor system or service functionality. Note: Please either avoid acronyms or expand acronyms, and please explain the functionality in such a way that it can be understood by someone who may not have a specific background or training on a business process, treatment methodology, technology, etc.	**Multimodality IVUS/FFR equipment** This device is used within a hospital setting to provide real-time internal blood pressure and ultrasonic imaging data of coronary and peripheral arteries.
What is the nature of the data to be stored, processed, or transmitted by the Vendor system or service? Select all that apply.	☐ **Confidential information (business sensitive data, intellectual property)** ☒ **Personally Identifiable Information (PII)** ☒ **Protected Health Information (PHI)/Patient Data*** ☐ **Payment Card Information (PCI) / Cardholder Data** ☐ **Other Data, specify:** Click here to enter text.
	***If PHI was checked above, will the Vendor sign (or has the Vendor signed) a Business Associates Agreement (BAA) with Providence in compliance with the Healthcare Information Accountability and Portability Act (HIPAA)?** ☒ **Yes** ☐ **No** **Comment: Boston Scientific does not handle any PHI/PII data. All data is stored locally and controlled by the hospital.**
Is all or part of the Vendor solution considered a Medical Device as defined by the United States Food and Drug Administration (FDA)?	☒ **Yes*** ☐ **No**
	***If the answer to this questions was Yes, please provide the following:** ☒ **FDA Certification #:** K201713 ☒ **Attach the corresponding MDS2 and return it along with this form or document why an MDS2 has not been completed.**
Where will Providence data reside, both logically and physically? Select all that apply.	☒ **Providence Hosted Server and/or System** ☐ **Vendor Data Center** ☐ **A Cloud Provider Service (SaaS, PaaS, IaaS) or hosted service** ☐ **Other, specify:** Click here to enter text.

In which geographies will Providence data be stored, processed, transmitted, or accessed?	☒ **Within the legal borders of the United States** ☐ **Outside the legal borders of the United States ("offshore")** Please list the corresponding locations outside the US: Click here to enter text.
Which of the following technologies can be used with the Vendor system or service? Select all that apply.	☐ **Workstation/Laptop (Windows)** ☐ **Mac OS Systems** ☐ **Mobile Devices (Android or iOS-based tablets, smartphones, etc.)** ☒ **Server (PACS, MWL)** ☐ **Cloud** ☐ **IoT (Internet of Things devices: non-workstation network-connected peripheral devices like smart-watches, thermostats, etc.)** ☒ **Other technologies, specify: Tablet-based multimodality guidance system partnered with our OptiCross HD / OptiCross Imaging Catheters and COMET II Pressure Guidewire - Additional Components: FFR Link, Motor Drive Unit, LCD Monitor Display, Acquisition PC, Wireless mouse / keyboard options)**
Will this system or service appropriately function without the use of Internet Explorer?	☐ **Yes** ☐ **No** ☒ **N/A – System or service does not use a web browser**
Will this system or service fully function when using the Microsoft Chromium Edge browser?	☐ **Yes** ☐ **No** ☒ **N/A – System or service does not use a web browser**
Who will support this system or service (e.g., patching, upgrading software, and/or workstation or device security)? Select all that apply?	☒ **Vendor** ☐ **Providence** ☐ **Providence & Vendor hybrid** ☐ **Other, specify:** Click here to enter text.

Payment Card Industry (PCI)

Will the system or service store, process, or transmit Payment Card Industry (PCI) / Cardholder Data (e.g., credit or debit card information)?

☐ Yes – Answer the questions below and supply the information and documents requested below to Providence when returning this form.

☒ No – Skip this section and proceed to the next section

PCI – Complete all fields below. If you are uncertain about how to answer a question, please contact the assigned security analyst or the Providence point of contact.

#	Question	Response	Vendor Comments / Written Response	Providence Comments
PCI 0.1	Will the Vendor solution incorporate any components that will be installed on a Providence network or Providence-managed cloud subscription (e.g., Azure, AWS, GCP)?	**☐ Yes** **☐ No**		
PCI 0.2	For solutions that involve physical payment devices, are the devices owned by __________?	**☐ Providence** **☐ Vendor** **☐ Other**	If "Other", please specify below:	
PCI 0.3	For solutions that involve physical payment devices, are the devices ordered and maintained by ________?	**☐ Providence** **☐ Vendor** **☐ Other**	If "Other", please specify below and include contact information needed for ordering and/or maintaining the device:	
PCI 0.4	For solutions that involve physical payment devices, please provide the following:		Device Model: Click here to enter text. Manufacturer: Click here to enter text.	

#	Question	Response	Vendor Comments / Written Response	Providence Comments
			Software name and version: Click here to enter text.	
PCI 0.5	What payment processor or gateway will be used?			
PCI 0.6	Please provide all of the following supporting documentation and return it to Information Security along with this form: ☐ Attestation of PCI compliance from the vendor. ☐ Diagram of how credit card data flows from Providence to the Vendor's system. ☐ As applicable, verification that the Vendor is hosting the website and payment page, the entire credit card process (to include encryption during transit), and the storage and security of credit card information.			

1. Administrative, Policy, and Procedure: DO NOT SKIP

'No' or 'N/A' answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
1.1	Does the Vendor have and proactively maintain a current HIPAA-compliant Privacy policy that clearly documents requirements for identifying, classifying and maintaining the confidentiality of Protected Health Information (PHI)? (IMPORTANT: If the Vendor will not store, process, transmit, or otherwise access PHI, as defined by HIPAA, please respond with an 'N/A'. Also, include a comment noting that the	☐ Yes ☐ No ☒ N/A	Data remains locally	

#	Question	Response	Vendor Comments	Providence Comments
	Vendor will not store, process, transmit or otherwise access Providence PHI.)			
1.2	Does the Vendor have and proactively maintain a current security policy that adheres to specifications documented in any of the following? • NIST 800 series • ISO 27000 series • HITRUST • HIPAA	☐ **Yes** ☒ **No**		FDA device registration # is K201713. MDS2 document has been provided as evidence.
1.3	Does the Vendor continuously monitor for new and updated regulations to ensure their product's continued compliance with applicable laws, regulations and best practices?	☒ **Yes** ☐ **No** ☐ **N/A**		
1.4	Does the Vendor have a formal, comprehensive information security program that includes security governance, security risk management and operational security disciplines?	☒ **Yes** ☐ **No**	Boston Scientific has an extensive information security program. There are GRC teams at Local, State, Regional, and Global levels.	
1.5	Does the Vendor have a designated information security officer, or equivalent function, to coordinate, develop, implement, and maintain its Information Security program?	☒ **Yes** ☐ **No**	Same as above, there are designated leaders in each locality that partner with Business units to ensure comprehensive coverage.	
1.6	Does the Vendor clearly define and assign information security responsibilities to designated staff within its organization?	☒ **Yes** ☐ **No**		
1.7	Does the Vendor have a formal information security training and awareness program?	☒ **Yes** ☐ **No**		
1.8	Is information security training required for all employees and workforce members who could access Providence data?	☒ **Yes** ☐ **No**	All employees must conduct infosec training with specialized training depending on their duties. No Boston Scientific employee will have access to Providence data. Field Service Engineers access	

#	Question	Response	Vendor Comments	Providence Comments
			the system physically and can access system logs and the underlying operating system only.	
1.9	Does the Vendor perform background checks on individuals handling or otherwise accessing Providence's information or information systems?	☒ Yes ☐ No	Boston Scientific conducts back ground checks on all employees and require them to be properly credentialed to enter hospitals.	
1.10	Does the Vendor require its workforce members to agree to and sign a document addressing the terms and conditions of their employment and a workforce member's: • Acknowledgement of the acceptable use of information and information systems, • Responsibilities for securing and protecting confidential information, • Responsibilities to report potential security events that involve confidential information?	☒ Yes ☐ No		
1.11	Does the vendor have a timely process to revoke access to their employees and contractors who have left the organization? (Note: This revocation process should not exceed 24 hours when staff leave under amicable conditions, and revocation should be immediate for staff terminated under adverse conditions.)	☒ Yes ☐ No		

2. Development Practices: DO NOT SKIP

'No' or 'N/A' answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
2.1	Does the Vendor's organization adhere to a formal security development methodology, like Microsoft SDL,	☒ Yes ☐ No	Secure software development process, such as ISO/IEC 27034 or	

#	Question	Response	Vendor Comments	Providence Comments
	OWASP OpenSAMM, or BSIMM? Or, at a minimum, does the Vendor organization build formal security requirements and checkpoints into the development process?	☐ **N/A**	IEC 62304, followed during product development	
2.2	Does the Vendor secure source code and limit access to only authorized individuals?	☒ **Yes** ☐ **No** ☐ **N/A**		
2.3	Does the Vendor prohibit the use of production data in non-production environments?	☒ **Yes** ☐ **No** ☐ **N/A**		

3. Access Control – General: DO NOT SKIP

‘No’ or ‘N/A’ answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
3.1	Does the Vendor system and/or service support authentication via a cloud-based Identity Provider solution (e.g., Ping, OKTA, Microsoft, etc.) for Single Sign On (SSO)?	☐ **Yes** ☐ **No** ☒ **N/A**	It is just standalone medical device system. Only local account authentication is used.	Will be connected to providence VLAN
3.2	Does the Vendor system and/or service support either Multi-Factor Authentication (MFA) or Two Factor Authentication (2FA)?	☐ **Yes** ☐ **No** ☒ **N/A**	It is just standalone medical device system. Only local account authentication is used.	
3.3	Does the system or service require a unique username (ID) and password?	☐ **Yes** ☐ **No** ☒ **N/A**	It is just standalone medical device system. Only local account authentication is used.	System comes with default account. Providence controls the accounts thereafter. Providence can set unique ID’s & passwords as per our policies
3.4	Does the system or service require that each administrator account have a unique username (ID) and password?	☐ **Yes** ☐ **No** ☒ **N/A**	Local account which hospital can create and admin can apply role based access	Refer to 3.3

#	Question	Response	Vendor Comments	Providence Comments
3.5	Can individual user sessions lock or be configured to lock (requiring a password before reuse) after 15 or fewer minutes of inactivity? (If the answer is 'No', use the comment field to indicate either an alternative lockout timeframe (e.g., 30 or 60 minutes) or a rationale for not locking a session after a period of inactivity.)	☐ Yes ☐ No ☒ N/A	Inactivity timeout setting is not available.	
3.6	Can default, published or otherwise disclosed system or service accounts be changed or deleted during or after installing or configuring the system/service for use at Providence?	☐ Yes ☐ No ☒ N/A	It's just a Local account which hospital can create and admin can apply role bases access.	See 3.3
3.7	Does the system or service mask passwords during entry, rendering contents in the password field unreadable?	☒ Yes ☐ No ☐ N/A	The Password entry field is masked so that all entered passwords are unreadable.	
3.8	Does the system or service support role-based access control?	☒ Yes ☐ No ☐ N/A	Local account which hospital can create and admin can apply role based access.	
3.9	Does the system or service support least privileged access? In other words, does the system or service facilitate presenting users with the minimum necessary data elements required to perform a job function?	☐ Yes ☐ No ☒ N/A		

4. Access Control – User Accounts

Are user accounts provisioned and managed using the Vendor system/service rather than Providence AD/LDAP integration or Providence's Identity Provider solution (e.g., Ping, OKTA, Microsoft, etc.)?

☐ **Yes – Answer the questions below**

☒ **No – Skip this section and proceed to the next section**

'No' or 'N/A' answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
4.1	Does the system or service natively perform the following, or can it be configured to do so?	☒ Yes ☐ No ☐ N/A	The system uses Bitlocker AES-256 to encrypt all hard drive data.	This device is designed to boot up directly into a sandboxed application

#	Question	Response	Vendor Comments	Providence Comments
	Following 10 or fewer failed login attempts: - Disable a user's account for at least 15 minutes - Lock a user's account for at least 30 minutes?			without any user intervention. Is used more like a Kiosk, ready to use.
4.2	Does the system or service natively adhere to the following, or can it be configured to do so? Passwords must have a minimum of 8 characters and contain 3 of the 4 criteria below: - At least 1 uppercase letter - At least 1 lowercase letter - At least 1 number - At least 1 symbol or special character (e.g., @, #, &, etc.)	☐ **Yes** ☐ **No** ☒ **N/A**		See 4.1
4.3	Does the system or service natively expire passwords after 365 days or fewer, or can Providence administrators custom configure password expiration parameters in accordance with Providence policy?	☐ **Yes** ☐ **No** ☒ **N/A**		See 4.1
4.4	Does the system or service natively prevent password reuse, or can Providence administrators custom configure password reuse requirements (e.g., prevent a user from using x number of prior passwords)?	☐ **Yes** ☐ **No** ☒ **N/A**		See 4.1
4.5	Does the system or service require users to reset their password upon initial login?	☐ **Yes** ☐ **No** ☒ **N/A**		See 4.1
4.6	Does the system or service transmit passwords from the browser (or other input form) to the back-end authentication mechanism using a minimum of protocol of TLS 1.2, and	☐ **Yes** ☒ **No**		

#	Question	Response	Vendor Comments	Providence Comments
	an encryption algorithm and strength of AES-256?			
4.7	Does the system or service cryptographically store passwords at rest using a salted non-reversible hash comprised of SHA2 or SHA3 with at least 10,000 salt iterations? (Acceptable hashing and salting mechanisms include PBKDF2, Balloon, bcrypt, or other industry-standard tools.)	☐ **Yes** ☒ **No**		

5. Cryptography: DO NOT SKIP

‘No’ or ‘N/A’ answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
5.1	Does the system or service transmit (internal and external) *all* data using a minimum protocol of TLS 1.2, and an encryption algorithm and strength of AES-256?	☐ **Yes** ☒ **No**	The system connects to specific ports and ip addresses for ntp and McAfee end point protection reporting and updates (See network diagram). No other connections are allowed. Internally, only Bluetooth connections to FFR links and DICOM to PACS/MWL. No patient data ever reaches out to the internet from this system. It can only leave the system using DICOM or physically via external usb drives. • Network access is currently through Ethernet only (DICOM) • Wi-Fi is disabled • IPv6 is blocked by the system’s firewall • All incoming communications are	. Accepting for this use case as there are many compensating controls provided by the vendor. Also the system is a Kiosk model.

#	Question	Response	Vendor Comments	Providence Comments
			blocked, as no externally-initiated communications are permitted • All unused ports are blocked • Outbound communications are restricted to a combination of known good hosts, ports, or originating processes	
5.2	Does the system or service DISABLE all versions of SSL and older versions of TLS, specifically TLS 1.0 and TLS 1.1?	☒ Yes ☐ No	See 5.1 comment, SSL and TLS is disabled on the system.	Same as 5.1
5.3	Unstructured Data: Does the system or service use a minimum of AES 256-bit encryption to protect *all* stored confidential or regulated data on *all* servers, NAS devices, workstations, mobile systems, devices, files shares, portable media, and any other component of the system or service that is used to store Providence information?	☒ Yes ☐ No	Hard Drive Encryption- BitLocker 256 AES	
5.4	Structured Data: Are *all* structured data stores (databases) or database fields that store Providence confidential or regulated information encrypted using a minimum of AES-256 bit encryption? (IMPORTANT: If the answer is 'No' or 'N/A', either use the comment field to document the alternate encryption algorithm and strength that is used instead of AES-256, or to document the rationale for not encrypting data.)	☒ Yes ☐ No	The system doesn't use databases or structured data to archive images. But yes, all data is encrypted with Bitlocker.	
5.5	Are cryptographic keys stored in a secure key vault that protects keys from unauthorized access and use?	☒ Yes ☐ No	The full volume encryption key is encrypted by the volume master key and stored in the encrypted drive. The volume master key is encrypted by the	

#	Question	Response	Vendor Comments	Providence Comments
			appropriate key protector and stored in the encrypted drive. Trusted Platform Module (TPM) is utilized to store the decryption key	

6. Logging: DO NOT SKIP

‘No’ or ‘N/A’ answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
6.1	Are audit logs available for at least 90 days for non-PHI/regulated activities and one year for PHI related activities?	☐ Yes ☐ No ☒ N/A	N/A - It doesn’t have the capability to provide audit logs.	This device is designed to boot up directly into a sandboxed application without any user intervention. The only way to break out of this is to enter the admin password.
6.2	Does the system or service protect against log tampering by preventing non-administrative users from altering or deleting log content?	☒ Yes ☐ No ☐ N/A	It’s a hospital responsibility to manage access control.	
6.3	Do audit logs capture at least the following information: Successful logins, failed logins, data views, data modifications, and data deletions?	☒ Yes ☐ No ☐ N/A	Local sign-in activity, Upgrade history, Diagnostic events, Information events, Errors and Warnings	
6.4	Does the Vendor system maintain logs that record access to specific records within the application, including which user accessed the record and when?	☐ Yes ☐ No ☒ N/A	It doesn’t have the capability to provide audit logs	
6.5	Are all server modifications logged?	☐ Yes ☐ No ☒ N/A		It’s a PAC system, which is being managed by Providence.

7. Mobile Devices (Providence facilities or remote)

Will the Vendor solution, or components of solution, use mobile devices (iOS or Android systems) and/or a mobile app? (Note: mobile devices accessing a service through a web browser are not in scope for this question.)

☐ **Yes – Answer the questions below**

☒ **No – Skip this section and proceed to the next section**

‘No’ or ‘N/A’ answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
7.1	Does the Vendor's solution require users to enter a password, PIN, and/or biometric authentication mechanism in order to access mobile application content?	☐ **Yes** ☐ **No** ☒ **N/A**		
7.2	Does the mobile application time out after 15 or fewer minutes of inactivity, requiring a user to re-enter a password, PIN, or re-initiate a biometric authentication mechanism before app content can be viewed again?	☐ **Yes** ☐ **No** ☒ **N/A**		
7.3	Does the mobile app store data locally on the device in a containerized, encrypted state?	☐ **Yes** ☐ **No** ☒ **N/A**		
7.4	Can Providence or authorized administrators delete Providence data or render Providence data unreadable when an employee or workforce member's access is terminated?	☐ **Yes** ☐ **No** ☒ **N/A**		
7.5	Is the mobile application capable of single sign-on (SSO) through an online identity provider service (e.g., OKTA, Ping, Microsoft, etc.) or via LDAP/Active Directory?	☐ **Yes** ☐ **No** ☒ **N/A**		

8. On-premises (Providence facilities) or Providence-Managed Cloud Tenants Solutions

Will the Vendor solution, or components of solution, be installed on assets within Providence-managed facilities or cloud environments, such facilities or cloud environments include datacenters, Azure or AWS tenants, server closets, offices, clinical locations or any other Providence owned or leased facilities?

☐ **Yes – Answer the questions below**

☒ **No – Skip this section and proceed to the next section**

‘No’ or ‘N/A’ answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
8.1	Does the Vendor agree to use the Providence-provided VPN for remote access to the Providence network rather than Vendor remote access/support tools? (Providence currently uses Citrix for remote VPN support.)	☐ Yes ☐ No ☒ N/A	Not required.	
8.2	For times when the Vendor must access the Providence network (including Providence cloud tenants) to fulfill obligations under the Master Services Agreement or other contractual obligations, will only United States-based Vendor personnel and resources access Providence networks, network assets, cloud tenants, data, and information systems?	☐ Yes ☐ No ☒ N/A	It's a standalone medical device.	
8.3	Will all servers, workstations and/or other components of the Vendor's solution run on an operating system (OS) that is currently supported by the OS vendor or open source community?	☐ Yes ☐ No ☒ N/A	Windows 10 IoT Enterprise version 1809 is the device OS and the image is maintained by Boston Scientific.	
8.4	Can the OS or OSs supporting the Vendor's system(s) be updated to a newer version when the current OS approaches end of support?	☒ Yes ☐ No ☐ N/A	It "can" be updated to a newer version, but the timeline would be based on Boston Scientific development not Microsoft support.	
8.5	Can Providence manage updates on the server, workstation, and/or other device's OS?	☐ Yes ☒ No ☐ N/A	The device require vendor or vendor-authorized service to install patches or software updates	Providence will only co-ordinate, Vendor needs to update, patch etc
8.6	Can Providence manage updates on third Party applications (non-OS applications such as Adobe Acrobat, web browsers, etc.)?	☐ Yes ☐ No ☒ N/A	It is just standalone medical device.	
8.7	Can the Vendor's solution be deployed and operationalized in a configuration where the application and data storage	☐ Yes ☐ No		This device is designed to boot up directly into a sandboxed application

#	Question	Response	Vendor Comments	Providence Comments
	components (e.g., databases or file storage systems) can reside and operate on separate physical or virtual servers?	☒ **N/A**		without any user intervention. Is used more like a Kiosk, ready to use.
8.8	Can data stores (e.g., databases or file storage systems) containing confidential or regulated information be logically located in a secure network segment that is separated (by a firewall or restrictive ACLs) from application servers, workstations, and other system components?	☐ **Yes** ☐ **No** ☒ **N/A**	Data store locally and remains under hospital premises.	Data is stored in Providence VLAN
8.9	Can Providence administrators install a Providence-managed anti-malware client (running real-time scanning on a continuous basis) on the Vendor solution's servers, workstations, and/or other applicable devices? (If YES, list all directories and file types that must be excluded by the anti-malware client.)	☐ **Yes** ☒ **No** ☐ **N/A**	[**Comment required for 'Yes' answers on this question**]:	
8.10	Can Providence administrators install a Providence-managed host-based firewall client on the Vendor solution's servers, workstations, and/or other applicable devices?	☐ **Yes** ☒ **No** ☐ **N/A**		
8.11	Can Providence conduct system backups using a method of Providence's choosing, including encrypting any backups?	☐ **Yes** ☐ **No** ☒ **N/A**	No backup required since data stored locally.	Data is stored on PACS server in Providence
8.12	Can Providence conduct credentialed/authenticated vulnerability scans on all Vendor servers and other Vendor systems without disrupting the operations of these systems?	☐ **Yes** ☐ **No** ☒ **N/A**		Providence has a Vulnerability Scan program in place, providence managed servers are part of this program.
8.13	Can the Vendor solution be deployed so that end users do not need local administrative privileges on workstations or systems running the application?	☐ **Yes** ☐ **No** ☒ **N/A**		

#	Question	Response	Vendor Comments	Providence Comments
8.14	Can Providence either install full disk encryption software on servers and/or workstations, or does the Vendor provide full disk encryption capabilities as part of its solution?	☐ Yes ☐ No ☒ N/A	Hard Drive Encryption-BitLocker 256 AES	
8.15	Does the system or service delete regulatory or other confidential information from local storage, temporary files, and memory upon logging out of or shutting down the application?	☐ Yes ☒ No ☐ N/A	• After archiving patient data, records are automatically deleted after six months • Patient data can be manually deleted at any time • Boston Scientific recommends deleting all patient data before returning the tablet for repairs or moving to another clinic or hospital	
8.16	Can logs be sent to or retrieved by the Providence SIEM by using a standard log format?	☐ Yes ☒ No ☐ N/A		
8.17	In the event of a zero-day or other emerging critical vulnerability, does the vendor either notify customers or provide documentation about which models, firmware versions, etc. may be impacted, and which patches, interim or indefinite compensating controls, or other corrective measures can be implemented to address the risk?	☒ Yes ☐ No ☐ N/A		
8.18	Does the Vendor provide documentation that indicates which services and ports are needed for the solution to operate effectively?	☒ Yes ☐ No ☐ N/A		
8.19	Can vulnerable protocols such as FTP, TFTP, Telnet, VNC, etc. be disabled?	☒ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
8.20	Can either Providence or the Vendor disable non-essential services and unneeded ports?	☒ Yes ☐ No ☐ N/A		
8.21	Does the Vendor or a Vendor-contracted third-party (subcontractor) test the system or service for security vulnerabilities? (**IF YES**, please list the frequency of these tests in the Vendor Comments section.)	☒ Yes ☐ No ☐ N/A	A third party is used for penetration testing the system before production release. They are also used prior to system updates being approved for release. Updates are done as needed, with no set schedule.	
8.22	Does the system or service exclude hard-coded passwords?	☒ Yes ☐ No ☐ N/A		

9. Cloud or Vendor Hosted Security

Will the Vendor solution, or components of the solution, be Software as a Service (SaaS) or a Vendor hosted service?

☐ **Yes – Answer the questions below**

☒ **No – Skip this section and proceed to the next section**

‘No’ or ‘N/A’ answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
9.1	Are development, test, and production environments separated from each other either logically or physically?	☐ Yes ☐ No ☒ N/A		
9.2	Is a formal change management procedure documented and implemented?	☐ Yes ☐ No ☒ N/A		
9.3	Are system and application patches applied in accordance with the following timelines:	☐ Yes ☐ No ☒ N/A		

#	Question	Response	Vendor Comments	Providence Comments
	• <24 hours for "Zero Day" (i.e., vulnerabilities that are being actively exploited in the wild) • <30 days for critical and high-risk vulnerabilities (on all systems and applications) • <30 days for medium-risk vulnerabilities on Internet-facing systems and applications • <60 days for medium-risk vulnerabilities on Internally-facing systems and applications			
9.4	Are vulnerability scans conducted against all internal and external systems and applications at least quarterly and after any significant system or application changes? (Examples of vulnerability scans include host and application scanning conducted by an industry-standard scanning tool or service like, but not limited to, Qualys, Rapid7, or Tenable Nessus.)	☐ **Yes** ☐ **No** ☒ **N/A**		
9.5	Are critical, high, and medium risk vulnerability scan findings remediated within a clearly defined and documented timeframe that does not exceed 30 days for critical, high-risk, and Internet-facing medium-risk vulnerabilities, and 60 days for all other medium-risk vulnerabilities?	☐ **Yes** ☐ **No** ☒ **N/A**		
9.6	Does the Vendor conduct, or contract, penetration testing on all external facing components of their production environment at least annually or after any significant system or service changes?	☐ **Yes** ☐ **No** ☒ **N/A**		
9.7	Are critical, high, and medium risk penetration test findings remediated within a clearly defined and documented timeframe that does not	☐ **Yes** ☐ **No** ☒ **N/A**		

#	Question	Response	Vendor Comments	Providence Comments
	exceed 30 days for critical, high-risk, and Internet-facing medium-risk vulnerabilities, and 60 days for all other medium-risk vulnerabilities?			
9.8	Is the hosted environment deployed with a network firewall at the perimeter that is configured to address security risks at Layers 3, 4, and 5 of the OSI Model?	☐ Yes ☐ No ☒ N/A		
9.9	Is the service architected with a minimum of three separate tiers: web services, application, and storage/database?	☐ Yes ☐ No ☒ N/A		
9.10	Is the hosted service's architecture configured in such a way that data stores (e.g., databases or file storage systems) containing confidential or regulated information are logically located in a secure network segment that is separated from application servers, web servers, workstations, the Internet, and other systems by a firewall or restrictive ACLs?	☐ Yes ☐ No ☒ N/A		
9.11	Is the hosted service's architecture deployed and configured in such a way that there is a web application firewall to protect the application (primarily Layer 7, but other layers as applicable) components of the service?	☐ Yes ☐ No ☒ N/A		
9.12	Are network intrusion detection systems / intrusion prevention systems (IDS/IPS) in place and configured to detect threats and protect the environment from attack?	☐ Yes ☐ No ☒ N/A		
9.13	Does the Vendor actively monitor their cloud/hosted services environment (in real or near real-time) for security incidents?	☐ Yes ☐ No ☒ N/A		
9.14	Does the Vendor have an established security incident management program that complies with legal and regulatory	☐ Yes ☐ No		

#	Question	Response	Vendor Comments	Providence Comments
	requirements related to incident/breach reporting and notification?	☒ **N/A**		
9.15	Does the Vendor have dedicated security staff used for responding to security incidents?	☐ **Yes** ☐ **No** ☒ **N/A**		
9.16	Is there a security incident notification process for notifying Providence of a security event that could adversely impact system availability or adversely impact the confidentiality or integrity of Providence data?	☐ **Yes** ☐ **No** ☒ **N/A**		
9.17	Do the Vendor's policies, standards, and service configurations prohibit storing confidential or regulated data in any external/internet-facing network segment?	☐ **Yes** ☐ **No** ☒ **N/A**		
9.18	Will Providence confidential and/or regulated data be accessed or administered by Vendor personnel exclusively within the United States?	☐ **Yes** ☐ **No** ☒ **N/A**		
9.19	Are information security requirements embedded within the Vendor's Business Continuity and Disaster Recovery Plans and Processes?	☐ **Yes** ☐ **No** ☒ **N/A**		
9.20	Does the Vendor maintain a current, formal certification or compliance report related to any of the following certifications or assessments? • ISO 27001 Certification • HITRUST Certification • FedRAMP Ready • FedRAMP Authorized • SSAE 16 or 18 SOC 2 Report	☐ **Yes** ☐ **No** ☒ **N/A**		
9.21	Does the Vendor encrypt and physically secure all system backup media that contains Providence data?	☐ **Yes** ☐ **No** ☒ **N/A**		

#	Question	Response	Vendor Comments	Providence Comments
9.22	Has the Vendor implemented procedures and controls to safeguard its datacenter facility and equipment from unauthorized physical access or theft, or does the Vendor use a public cloud service provider (e.g., AWS, Azure, GCP, etc.) that implements such physical security procedures and controls?	☐ Yes ☐ No ☒ N/A		
9.23	Does the Vendor log physical access to facilities that contain Providence information, or does the Vendor use a public cloud services provider (e.g., AWS, Azure, GCP, etc.) that logs physical access to its facilities that contain Providence information?	☐ Yes ☐ No ☒ N/A		

10. Vendor Back-Office Security

Will Providence data be stored, processed or transmitted within the Vendor's back-office, or Vendor company internal network, environment?

(**Note**: Most Vendors will skip this section, unless the Vendor stores, processes, or transmits Providence data on their office network rather than a dedicated cloud service or data center hosting environment. Only complete this section if Providence data will be stored, processed, or transmitted in a back-office network environment—meaning the environment that provides connectivity to the Vendor's workstations, mobile devices, or servers that are used to support the daily operations of its business, like emails, web browsing, conference calls, and misc. core business applications.)

☐ **Yes – Answer the questions below**

☒ **No – Skip this section and proceed to the next section**

'No' or 'N/A' answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
10.1	Has the Vendor implemented a formal asset management program, including inventory of authorized devices and software?	☐ Yes ☐ No ☒ N/A		
10.2	Has the Vendor implemented procedures and controls to safeguard its facility and equipment from unauthorized physical access or theft?	☐ Yes ☐ No ☒ N/A		

#	Question	Response	Vendor Comments	Providence Comments
10.3	Does the Vendor have a procedure for addressing lost devices such as laptops, cell phones, tablets, etc.?	☐ Yes ☐ No ☒ N/A		
10.4	Does the Vendor have physical security controls such as card control entry, security cameras, and uniformed security officers?	☐ Yes ☐ No ☒ N/A		
10.5	Does the Vendor log physical access to facilities that contain Providence confidential and/or regulated data?	☐ Yes ☐ No ☒ N/A		
10.6	Does the Vendor use Enterprise secure wireless protocols for controlling access to wireless networks?	☐ Yes ☐ No ☒ N/A		
10.7	Are server closets or smaller datacenters that host systems that store, process, or transmit Providence confidential or regulated data physically secured using locks, cameras, or other physical security controls? (If "other physical security controls" are used, please explain those in the Vendor Comments section.)	☐ Yes ☐ No ☒ N/A		
10.8	Does the Vendor log and monitor access to any server closets or smaller datacenters that host systems that store, process, or transmit Providence confidential or regulated data?	☐ Yes ☐ No ☒ N/A		
10.9	Are workstations and servers protected by host-based anti-malware applications?	☐ Yes ☐ No ☒ N/A		
10.10	Are workstations and servers protected by host-based intrusion detection and protection applications?	☐ Yes ☐ No ☒ N/A		

#	Question	Response	Vendor Comments	Providence Comments
10.11	Are workstations and servers protected by host-based firewalls?	☐ Yes ☐ No ☒ N/A		
10.12	Does the corporate network reside behind a network firewall that separates the corporate network from the Internet and other less secure networks or online services?	☐ Yes ☐ No ☒ N/A		
10.13	Are activities on the corporate network monitored by a Security Operations Center (or equivalent function) that is staffed and equipped with people, processes and technologies to rapidly respond to and remediate information security events?	☐ Yes ☐ No ☒ N/A		
10.14	Has the Vendor deployed data-loss prevention technologies that can detect and block attempts to exfiltrate confidential or regulated data?	☐ Yes ☐ No ☒ N/A		
10.15	Does the Vendor encrypt and physically secure all workstations, laptops, mobile devices and portable media that are used to store, process or transmit Providence confidential or regulated information?	☐ Yes ☐ No ☒ N/A		
10.16	Does the Vendor use Internet filtering technologies that block access to known malicious websites and website categories that might represent a security risk to Providence confidential or regulated data?	☐ Yes ☐ No ☒ N/A		
10.17	Does the Vendor use mobile device management technologies that manage the security on company-owned and employee-owned mobile devices used to store, process or transmit Providence confidential or regulated information?	☐ Yes ☐ No ☒ N/A		

#	Question	Response	Vendor Comments	Providence Comments
10.18	Does the Vendor centrally configure and manage secure configurations on their corporate workstation and server environment using tools like Active Directory, JAMF, or similar technologies?	☐ Yes ☐ No ☒ N/A		
10.19	Does the Vendor patch its corporate network assets (workstations, servers, appliances, etc.) in accordance with the following timelines: • <24 hours for "Zero Day" (i.e., vulnerabilities that are being actively exploited in the wild) • <30 days for critical and high-risk vulnerabilities (on all systems and applications) • <30 days for medium-risk vulnerabilities on Internet-facing systems and applications • <60 days for medium-risk vulnerabilities on Internally-facing systems and applications	☐ Yes ☐ No ☒ N/A		
10.20	Does the Vendor conduct vulnerability scans on all internet-facing corporate network assets at least quarterly?	☐ Yes ☐ No ☒ N/A		
10.21	Does the Vendor conduct credentialed/authenticated vulnerability scans on all internal corporate network assets at least quarterly?	☐ Yes ☐ No ☒ N/A		
10.22	Does the Vendor remediate discovered vulnerabilities within the following timelines: • <24 hours for "Zero Day" (i.e., vulnerabilities that are being actively exploited in the wild) • <30 days for critical and high-risk vulnerabilities (on all systems and applications)	☐ Yes ☐ No ☒ N/A		

#	Question	Response	Vendor Comments	Providence Comments
	• <30 days for medium-risk vulnerabilities on Internet-facing systems and applications • <60 days for medium-risk vulnerabilities on Internally-facing systems and applications			
10.23	Does the Vendor logically deploy data stores (e.g., databases or file storage systems) containing confidential or regulated information within in a secure network segment that is separated (by a firewall or restrictive ACLs) from workstations and other less secure system components?	☐ **Yes** ☐ **No** ☒ **N/A**		
10.24	Does the Vendor conduct security assessments on their business partners and any other Vendor that will directly or indirectly interact with Providence confidential or regulated data?	☐ **Yes** ☐ **No** ☒ **N/A**		
10.25	Does the Vendor use an email filtering technology to protect its network against phishing, malware, and other email-based attacks?	☐ **Yes** ☐ **No** ☒ **N/A**		
10.26	Does the Vendor have a threat intelligence team, or similar function, that continuously monitors external threat feeds and other sources for information about new cyber threats and mechanisms for defending against them?	☐ **Yes** ☐ **No** ☒ **N/A**		

11. Downstream Third-Party Vendors or Business Associates

Will Providence data be stored, processed, transmitted, or accessed by a Vendor subcontractor?

(Note: In the questions below, "Subcontractor" means any individual, corporation, partnership, joint venture, limited liability company, or other such entity that is, at any time during the term of an agreement with Providence, performing work on behalf of the Primary Vendor (meaning the company or organization completing this assessment questionnaire.)

☐ **Yes – Answer the questions below**

☒ **No – Skip this section and proceed to the next section**

‘No’ or ‘N/A’ answers require an explanation in the Vendor Comments field

#	Question	Response	Vendor Comments	Providence Comments
11.1	Prior to initiating the services of a Subcontractor, does the Vendor conduct an information security assessment on Subcontractor solutions or services that could impact Providence data (i.e., where the Subcontractor solution or service will involve the storage, processing, transmission, or access of Providence data)?	☐ **Yes** ☐ **No** ☒ **N/A**		
11.2	Does the Vendor also conduct periodic information security reassessments of Subcontractor solutions or services throughout the duration of the contract with the Subcontractor?	☐ **Yes** ☐ **No** ☒ **N/A**		
11.3	For times when the Vendor’s Subcontractors must access the Providence network or data (including Providence cloud tenants) to fulfill obligations under the Subcontractor agreement or other contractual obligations, will only United States-based Vendor personnel and resources access Providence networks, network assets, cloud tenants, data, and information systems?	☐ **Yes** ☐ **No** ☒ **N/A**		
11.4	For times when the Vendor’s Subcontractor must access resources or data on the Providence network or cloud environment, will the Vendor agree to ensure that Subcontractors will use only the Providence-provided VPN for remote access to the Providence resources (rather than Vendor or Subcontractor remote access/support tools)? (Providence currently uses Citrix for remote VPN support.)	☐ **Yes** ☐ **No** ☒ **N/A**		
11.5	Does the Vendor ensure that the Subcontractor signs a Business	☐ **Yes**		

#	Question	Response	Vendor Comments	Providence Comments
	Associates Agreement (BAA) for Subcontractor solutions or services that will or may store, process, transmit, or access Providence regulated Protected Health Information (PHI)?	☐ No ☒ N/A		
11.6	Does the Vendor hold Subcontractors contractually accountable to provide sufficient information security safeguards consistent with the NIST Cybersecurity Framework or other industry-recognized cybersecurity framework, including the identification and remediation of threats and vulnerabilities, in order to address security risks and threats (and assure HIPAA compliance, but only if PHI is involved)?	☐ Yes ☐ No ☒ N/A		

STOP

The last section is to be filled out by Providence Enterprise Information Security. If you have answered all of the above questions to the best of your knowledge, please send this form and any supporting documents to your assigned Providence Information Security Representative or primary Providence stakeholder.

*** * * Items below are to be completed by Providence Information Security * * ***

General Information:

Analyst Information	
EIS Analyst Name: Roza Reddy	**EIS Analyst Title: IT Risk Manager**
Date Assessed: 10.11.2022	**Peer Reviewer (Optional): Dave Thompson**
Business Stakeholder Ownership and Use Information	
Providence Owner Name: Justin E Gilbert	**Providence Contract Manager or Project Manager:** Click here to enter text.
Business Unit: Clinical Engineering	**Providence C-Level Sponsor: Cau Le**
Location where the system or service will be used:	**☐ Enterprise (used throughout Providence)** **☒ Specific Providence Location or Ministry, list all that apply:** • **PACS Server in Providence**

Review Rating:

Item	Area	Status
1	Security Within Providence's Environment	☒ Satisfactory ☐ Satisfactory with Conditions ☐ Fail ☐ N/A
2	Hosted Application Security	☐ Satisfactory ☐ Satisfactory with Conditions ☐ Fail ☐ N/A

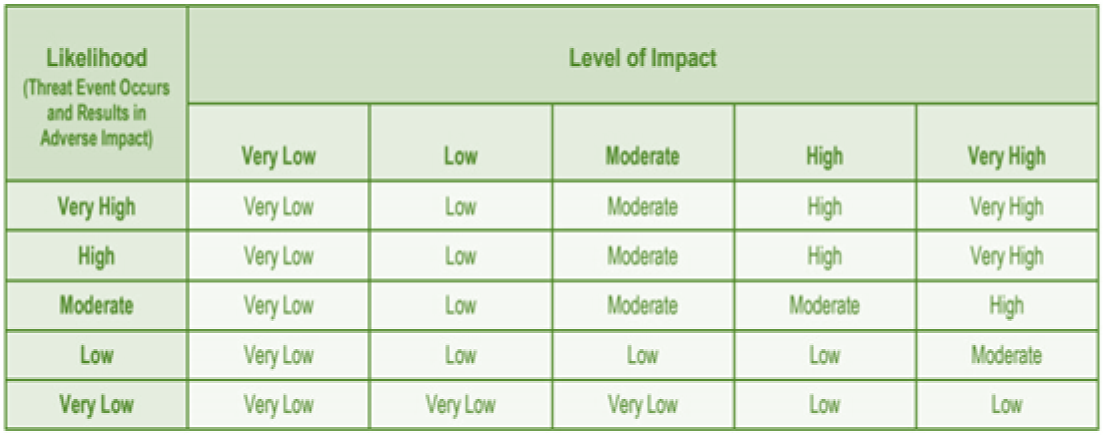
Document findings, risk, and any relevant recommendations or notes related to the review:

Review Summary:	
☒ **Satisfactory**	Providence Enterprise Information Security (EIS) conducted a review of Boston Scientific Corporation "Avvigo II IVUS/FFR system" and assigned a **Satisfactory** rating based on the responses and information provided by the Vendor. The assessment did not result in material findings, and the system or service is cleared for use. **Important**: Even with a Satisfactory rating, not all features within a system or service will be consistent with Providence requirements (i.e., policies, standards, regulatory requirements, contractual and legal obligations, and relevant federal, state, and local laws). Any such features and configurations that do not comply with Providence requirements cannot be used, except when a formal, documented exception has been issued by EIS. Providence Security Policies and Standards can be accessed on the EIS internal Intranet Page. Any questions about whether a specific configuration or feature is permissible can be directed to the security analyst assigned to this review, or by contacting InfoSecRiskAdvisory@providence.org.
☐ **Satisfactory with Conditions**	Providence Enterprise Information Security (EIS) conducted a review of **[System/Service Name]** and assigned a **Satisfactory with Conditions** rating based on the responses and information provided by the Vendor. The assessment resulted in some identified security risks that are registered in the findings section below. The Satisfactory with Conditions score means that the use of this system or service could adversely impact the confidentiality, integrity and availability of Providence systems or data. Providence EIS does not have assurance that the system or service can adequately protect Providence systems and data until the identified risks are adequately addressed. The key stakeholder (i.e., the business owner responsible for initiating and managing the Vendor relationship) is responsible determining whether the benefits associated with the use of this system or service outweigh the risks associated with its use, and such a decision may need

<table>
<tr><td></td><td colspan="2">to be in writing and accompanied by a formal, documented risk acceptance. Should the key stakeholder proceed with using the system or service despite his or her awareness of the risks, by doing so the key stakeholder is accepting the risks associated with its use and is responsible and accountable for any security and compliance incidents related to the use of the system or service. They key stakeholder is also responsible and accountable for working with the Vendor to remediate the risks identified as a result of this assessment, or to formally accept the risks if the Vendor cannot or will not address them.
Important: Even with a Satisfactory with Conditions rating, not all features within a system or service will be consistent with Providence requirements (i.e., policies, standards, regulatory requirements, contractual and legal obligations, and relevant federal, state, and local laws). Any such features and configurations that do not comply with Providence requirements cannot be used, except when a formal, documented exception has been issued by EIS.
Providence Security Policies and Standards can be accessed on the EIS internal Intranet Page. Any questions about whether a specific configuration or feature is permissible can be directed to the security analyst assigned to this review, or by contacting InfoSecRiskAdvisory@providence.org.</td></tr>
<tr><td>☐
Fail</td><td colspan="2">Providence Enterprise Information Security (EIS) conducted a review of **[System/Service Name]** and assigned a **Fail** rating based on the responses and information provided by the Vendor. The assessment determined that the system or service is not compliant with Providence requirements (i.e., policies, standards, regulatory requirements, contractual and legal obligations, and relevant federal, state, and local laws) and represents a material risk to Providence systems and/or data. Use of this system or service is not permitted.</td></tr>
<tr><td>**Observation #**</td><td>**Observation Description**</td><td>**Risk Rating and Tracking**</td></tr>
</table>

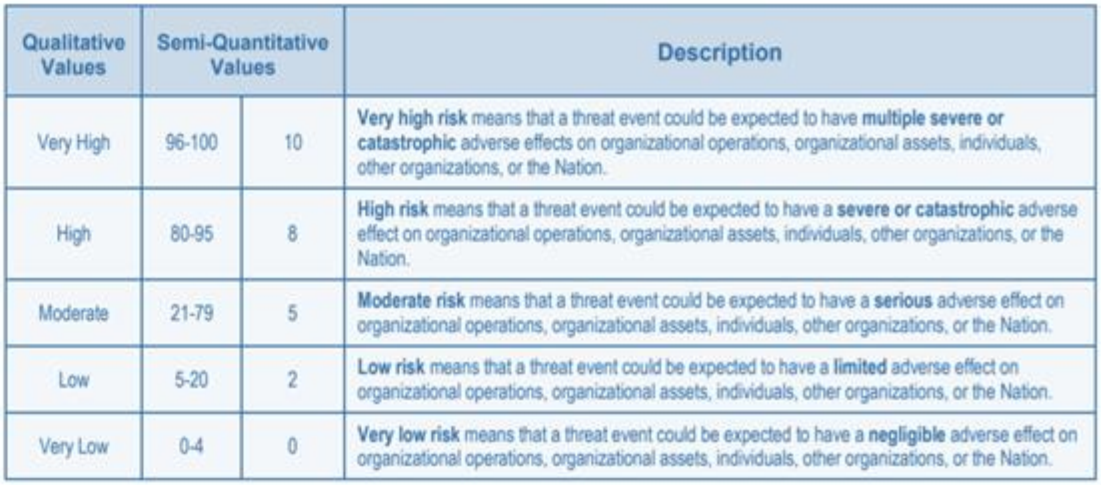
NIST Risk Tables:

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)



Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK



Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.