*** * * 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: 12/05/2022	**Vendor Company Name: Elekta, Inc.**
Vendor Contact Name: Maureen McCrary	**Product or Service Name(s): IntelliMax**
Vendor Contact Title: Strategic Proposals and GPO Administrator	**Vendor Website: www.elekta.com**
Vendor Contact Email: maureen.mccrary@elekta.com	**Vendor Support Phone Number:**
Vendor Contact Phone Number: Click here to enter text.	**Name of Primary Providence Stakeholder:** Click here to enter text.
Vendor Security Contact Information	
Security Contact Name: Click here to enter text.	**Security Contact Phone Number:** Click here to enter text.
Security Contact Title: Click here to enter text.	**Security Contact Email:** Click here to enter text.

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.	Click here to enter text. **IntelliMax Agent is a software program that is installed on a dedicated computer in the hospital. IntelliMax Agent is the only access point for Remote Access sessions from supported Elekta products out of the hospital network. IntelliMax Agent collects machine data from supported Elekta products, which it sends to IntelliMax Enterprise using a secure Internet connection. IntelliMax Agent does not collect patient data or PHI (Protected Health Information).** **IntelliMax Enterprise is used for the analysis of data collected by IntelliMax Agent. It is also used to administrator the Remote Access sessions to connected Elekta products. Approved users can get access to IntelliMax Enterprise through a web-based interface.**
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**
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 #:** Click here to enter text. ☐ **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: **Dublin Ireland, England UK**
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** ☐ **Cloud** ☐ **IoT (Internet of Things devices: non-workstation network-connected peripheral devices like smart-watches, thermostats, etc.)** ☐ **Other technologies, specify:** Click here to enter text.
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:			
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:			

#	Question	Response	Vendor Comments / Written Response	Providence Comments
	☐ 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 Vendor will not store, process, transmit or otherwise access Providence PHI.)	☐ **Yes** ☐ **No** ☒ **N/A**	Data is hosted by the customer.	Vendor documentation notes they will not transmit or store any PHI data, but vendor may 'see' information during a Remote Access session. Question marked N/A by the vendor.
1.2	Does the Vendor have and proactively maintain a current security policy that adheres to specifications documented in the NIST 800 series, ISO 27000 series, HITRUST, and/or HIPAA?	☒ **Yes** ☐ **No** ☐ **N/A**	ISO 17799	ISO 17799 renumbered to ISO 27002 in 2007
1.3	Does the Vendor maintain a current, formal certification or compliance report related to any of the following certifications or assessments?	☒ **Yes** ☐ **No** ☐ **N/A**	ISO 17799 Certification	

#	Question	Response	Vendor Comments	Providence Comments
	• ISO 27001 Certification • HITRUST Certification • FedRAMP Ready • FedRAMP Authorized • SSAE 16 or 18 SOC 2 Report			
1.4	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		
1.5	Does the Vendor have a formal, comprehensive information security program that includes security governance, security risk management and operational security disciplines?	☒ Yes ☐ No ☐ N/A		
1.6	Does the Vendor have a designated information security officer, or equivalent function, to coordinate, develop, implement, and maintain its Information Security program?	☒ Yes ☐ No ☐ N/A	Ramakrishnan Pillai	
1.7	Does the Vendor clearly define and assign information security responsibilities to designated staff within its organization?	☒ Yes ☐ No ☐ N/A		
1.8	Does the Vendor have a formal information security training and awareness program?	☒ Yes ☐ No ☐ N/A		
1.9	Is information security training required for all employees and workforce members who could access Providence confidential or regulated data?	☐ Yes ☐ No ☐ N/A		Question not answered by the vendor until receiving update via email on 9/12/22. Information Security training is provided at hire and at a minimum annually.
1.10	Does the Vendor perform background checks on individuals handling or otherwise accessing Providence's information or information systems?	☒ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
1.11	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 ☒ N/A	Data is hosted by the customer.	Question marked N/A by the vendor. Received update via email from Elekta on 9/12/22. Yes, Elekta does this but this does not apply when the data is hosted by the customer.
1.12	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 ☒ N/A	Data is hosted by the customer.	Question marked N/A by the vendor. Received update via email from Elekta on 9/12/22. Yes, Elekta does this but this does not apply when the data is hosted by the customer.

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, OWASP OpenSAMM, or BSIMM? Or, at a minimum, does the Vendor organization build formal security requirements and checkpoints into the development process?	☒ Yes ☐ No ☐ N/A		
2.2	Does the Vendor secure source code and limit access to only authorized individuals?	☒ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
2.3	Is confidential production data (i.e. real patient data, real credit card data, etc.) prohibited or de-identified (scrubbed/masked) from being used in any non-production environment (e.g. testing or development)?	☐ Yes ☐ No ☒ N/A	Real patient data is not stored by IntelliMax	Question marked N/A by the vendor. Acceptable response - Remote access and hardware support software. Vendor attests no PHI or Confidential information is collected or stored.

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		Solution does not comply with Providence's minimum security requirements. IntelliMax Agent is locally installed on Providence workstation, and does not have any specific login. Accessing the workstation requires Providence credentials. IntelliMax Enterprise Web only requires Single Factor Authentication and does not use SSO or MFA. IntelliMax Connect remote support connection to vendor is initiated from within Providence on IntelliMax Agent workstation by Providence caregivers.
3.2	Does the Vendor system and/or service support Multi-Factor Authentication (MFA)?	☐ Yes ☒ No ☐ N/A		Solution does not comply with Providence's minimum security requirements. IntelliMax Agent does not have any specific login. The application is locally installed on a workstation.

#	Question	Response	Vendor Comments	Providence Comments
				Accessing the workstation requires Providence credentials. IntelliMax Enterprise Web only requires Single Factor Authentication and does not use SSO or MFA. https://elekta.axeda.com Vendor response: MFA is not possible with the Axeda solution. We are transitioning to a new infrastructure and MFA will be part of this authentication from the beginning. Axeda capabilities will start to be deprecated from mid 2023.
3.3	Does the system or service require a unique username (ID) and password?	☒ **Yes** ☐ **No** ☐ **N/A**		
3.4	Does the system or service require that each administrator account have a unique username (ID) and password?	☒ **Yes** ☐ **No** ☐ **N/A**		
3.5	Can individual user sessions 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**		
3.6	Can default, published or otherwise disclosed system or service accounts be changed or deleted during or after	☐ **Yes** ☐ **No** ☒ **N/A**	IntelliMax software does not include any default or published accounts	N/A – Acceptable response

#	Question	Response	Vendor Comments	Providence Comments
	installing or configuring the system/service for use at Providence?			
3.7	Does the system or service mask passwords during entry, rendering contents in the password field unreadable?	☒ Yes ☐ No ☐ N/A		
3.8	Does the system or service support role-based access control?	☒ Yes ☐ No ☐ N/A		
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	Following 10 or fewer failed login attempts, can the system or service be configured to either disable an account for 15 minutes or lock users out for at least 30 minutes?	☒ Yes ☐ No ☐ N/A		
4.2	Can the system or service be configured to support the following password length and strength requirements? 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	☒ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
	• At least 1 symbol or special character (e.g., @, #, &, etc.)			
4.3	Can the system or service be configured to automatically expire passwords after a Providence-specified duration (e.g., 90 days)?	☒ Yes ☐ No ☐ N/A		
4.4	Can Providence configure password reuse requirements in the system or service (e.g., prevent a user from using x number of prior passwords)?	☐ Yes ☒ No ☐ N/A	Password re-use already restricted	System configured to require users change their password every 90 days.
4.5	Does the system or service require users to reset their password upon initial login?	☐ Yes ☒ No ☐ N/A		Initial password reset not required by vendor.
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 an encryption algorithm and strength of AES-256?	☒ Yes ☐ No ☐ N/A		
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 ☐ N/A		
4.8	Can password length requirements be configured such that privileged accounts and system/service accounts require a longer password than a general user account?	☐ Yes ☒ No ☐ N/A		Recommend vendor improve future iteration of the software to allow for longer password requirements for privileged accounts.

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) regulated or confidential data using a minimum protocol of TLS 1.2, and an encryption algorithm and strength of AES-256?	☐ Yes ☒ No ☐ N/A		Received update via email from Elekta on 9/12/22. Vendor updated initial response and noted data in transit is encrypted with TLS 1.2 with AES-256 bit encryption. Vendor security documentation notes that no PHI or PII is transferred from the hospital with the IntelliMax Agent. IntelliMax Agent only collects data from the Elekta products in relation to operation and status of the machine, not the patient in treatment. IntelliMax Connect Remote Access, clients give remote access to the graphical user interface of the medical product therefore the remote engineer can be exposed to PII.
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 ☐ N/A	In the process of updating to TLS 1.2	Vendor response 9/26: IntelliMax Agent does not use TLSv1.2 or below from Agent 4.2 on. This will be rolled out ~November 2022 Recommend vendor eliminate TLS versions less than TLSv1.2 from the operations of the software, as it exposes vulnerabilities within our network. Elekta documentation notes the remote screen-share data is transferred through an SSL tunnel from the IntelliMax Agent encapsulated using 256-bit

#	Question	Response	Vendor Comments	Providence Comments
				Secure Hash Algorithm (SHA2) encryption to the IntelliMax Enterprise Web. SSL. Vendor required a lot of back and forth questions during the investigation. May be additional risk not disclosed, as information was challenging to obtain.
5.3	Does the system or service use AES 256-bit full disk/device storage encryption on all servers, NAS devices, workstations, or mobile systems that store, process, or transmit regulated or confidential information?	☐ Yes ☒ No ☐ N/A	Workstations are not required to be encrypted by the system	Received update via email from Elekta on 9/12/22. Providence owned workstations should be encrypted by Providence. Vendor documentation notes that no PHI or PII is transferred or stored.
5.4	Are data stores (file systems or databases) containing regulated and other confidential information encrypted using AES-256 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 ☐ N/A	Access to the data can be limited to only the users that need access. Work is currently underway to make the data more secure.	Update via email from Elekta on 9/12/22. Data at rest is not encrypted. Vendor documentation notes that no PHI or PII is transferred from the hospital with the IntelliMax Agent. Requested additional clarification from the vendor on 8/15/22. Can the workstations be encrypted with BitLocker? Vendor Response 9/26: In theory yes. We have not seen this done before but would be interested in confirmation that everything works.

#	Question	Response	Vendor Comments	Providence Comments
				Providence owned workstations should be encrypted by Providence. Recommend vendor encrypt data at rest.
5.5	Are cryptographic keys stored in a secure key vault that protects keys from unauthorized access and use?	☐ Yes ☐ No ☐ N/A		Vendor Response 9/26. - No Question not originally answered by the vendor, , nor additional questions answered. Where are keys stored?

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		
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		
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	Data view is not audited	Elekta documentation notes the following: Elekta audit logs of who remotely started sessions. The customer can audit who started the session on their product (for linacs only). IntelliMax Enterprise provides an audit search capability for the above audit data. Elekta does not extract this audit data Elekta also audits files attempted to be transferred

#	Question	Response	Vendor Comments	Providence Comments
				through the client and successfully transferred files. No reports are produced using data from within a session. Logs are also captured for the success or failure of data extraction into Elekta Business Intelligence. No PHI is in any of the files or data fields according to their documentation. *Elekta does extract specific files and data for use in business intelligence to allow proactive service and predictive maintenance.*
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**		Received update from Elekta via email on 9/12/22. User behavior (viewing pages) is not logged, unless an action is performed that would result in a connect to a device. Recommend vendor update logs to include data view to record access to specific records within the application, including which user accessed the record and when.
6.5	Are all server modifications logged?	☐ **Yes** ☐ **No** ☐ **N/A**		No response from vendor. Received update from Elekta via email on 9/12/22. Server logging includes User Login/Logout events, Remote Session activity, as well as any significant system events or configuration changes.

#	Question	Response	Vendor Comments	Providence Comments
				Many questions were initially not answered by the vendor. Elekta has required a lot of back and forth questions during the investigation. May be additional risk not disclosed, as information was challenging to obtain.

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	☐ Yes		

#	Question	Response	Vendor Comments	Providence Comments
	identity provider service (e.g., OKTA, Ping, Microsoft, etc.) or via LDAP/Active Directory?	☐ **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**	VPN access not required for IntelliMax	Received update from Elekta via email on 9/12/22. Vendor does not agree to use Providence VPN for remote access. IntelliMax is their product intended to cover Elekta remote support and monitoring needs for some Elekta devices (eg Linacs) VNC is the underlying client/server that is used in IntelliMax Connect sessions for screen sharing. VNC is listed on Providence Denied Productivity and Developer Software. Denied Productivity and Developer Software (sharepoint.com) Vendor response: Providence VPN is not supported in a standard service contract and would require a non-standard process to be followed that

#	Question	Response	Vendor Comments	Providence Comments
				may impact the cost of service/compliance. Vendor update 9/26 Can IntelliMax Agent run independently to continue to provide health and status information? Yes, while not formally documented as separate things, IntelliMax Connect can be disabled and the IntelliMax Agent will continue to run. Simply blocking the GAS URLs would also provide this capability. Be aware our Service Agreements mandate the use of IntelliMax Connect to allow us to remotely support products, so other means of remote support will need to be investigated and could impact the service agreement costs.
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**	Service to confirm	No response. Question not answered by the vendor. IT Contracting should be informed of non-US geographies, to ensure appropriate legal provisions are included in the contract to protect Providence data. Vendor required a lot of back and forth questions during the investigation. May be additional risk not disclosed, as information was challenging to obtain.
8.3	Will all servers, workstations and/or other components of the Vendor's	☒ **Yes** ☐ **No**		

#	Question	Response	Vendor Comments	Providence Comments
	solution run on an operating system (OS) that is currently supported by the OS vendor or open source community?	☐ N/A		
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		
8.5	Can Providence manage updates on the server, workstation, and/or other device's OS?	☒ Yes ☐ No ☐ N/A		
8.6	Can Providence manage updates on third Party applications (non-OS applications such as Adobe Acrobat, web browsers, etc.)?	☒ Yes ☐ No ☐ N/A		
8.7	Can the Vendor's solution be deployed and operationalized in a configuration where the application and data storage components (e.g., databases or file storage systems) can reside and operate on separate physical or virtual servers?	☐ Yes ☒ No ☐ N/A		No comments from vendor. IntelliMax Agent specifically requires physical workstation, per Elekta documentation and cannot be installed on a virtual workstation desktop. IntelliMax Enterprise web is vendor hosted.
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		No comments from vendor. IntelliMax Agent is installed on a Providence workstation, which is then used to connect to some Elekta devices, and Elekta Enterprise Web.
8.9	Can Providence administrators install a Providence-managed anti-malware client (running real-time scanning on a	☒ Yes ☐ No		

#	Question	Response	Vendor Comments	Providence Comments
	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.)	☐ N/A		
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	Elekta recommends purchasing Direct Storage for backup but can use their own method.	
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		IntelliMax Enterprise Web is vendor hosted PaaS. IntelliMax Agent is installed on a Providence workstation.
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		
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	Providence can use disk level encryption	
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		No comments from vendor. Elekta documentation states no PHI or confidential information is stored or transferred.
8.16	Can logs be sent to a Providence SIEM in a standard log format such as syslog or LEEF?	☒ Yes ☐ No	Windows logs can be collected by customer	

#	Question	Response	Vendor Comments	Providence Comments
		☐ 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	VNC protocol is used for remote support	Received update from Elekta via email on 9/12/22. VNC is the underlying client/server that is used in IntelliMax Connect sessions for screen sharing. Recommend implementation team ensure vulnerable protocols are disabled. VNC is listed on Providence Denied Productivity and Developer Software. Denied Productivity and Developer Software (sharepoint.com)
8.20	Does the Vendor provide documentation describing how to disable vulnerable protocols, such as FTP, TFTP, Telnet, VNC, etc.	☐ Yes ☒ No ☐ N/A		Recommend Providence IS support team ensure vulnerable protocols are disabled.

#	Question	Response	Vendor Comments	Providence Comments
8.21	Can PSJH disable non-essential services and unneeded ports?	☒ Yes ☐ No ☐ N/A		
8.22	Does the Vendor or a Vendor-contracted third party 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	At minimum annually	
8.23	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	Are file-integrity monitoring tools in place to monitor modifications to critical system files, configuration files, and content files?	☒ Yes ☐ No ☐ N/A		
9.3	Is a formal change management procedure documented and implemented?	☒ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
9.4	Are system and application patches applied 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	We immediately access the urgency of all security patches for components of the IntelliMax solution, we would aim to apply these in line with the provided timescales, where this can be achieved with appropriate quality testing.	
9.5	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 Qualys, Rapid7, or Tenable Nessus.)	☐ Yes ☒ No ☐ N/A		Received update from Elekta via email on 9/12/22. Internal vulnerability assessments are performed by PTC Compliance personnel on a monthly basis to identify network vulnerabilities. Identified risks from the assessments are evaluated by management to determine the criticality and potential impact of the findings and actions are taken to correct the vulnerabilities (PTC is an Elekta Enterprise Web contracted vendor)
9.6	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	☒ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
	vulnerabilities, and 60 days for all other medium-risk vulnerabilities?			
9.7	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		Received update from Elekta via email on 9/12/22. A third-party information security vendor conducts external security penetration tests PTC hosted environments on at least an annual basis to identify vulnerabilities and potential exploits that may impact the security availability of the system
9.8	Are critical, high, and medium risk penetration test 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		Received update from Elekta via email on 9/12/22. Identified risks from the assessments are evaluated by management to determine the criticality and potential impact of the findings and actions are taken to correct the vulnerabilities
9.9	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		
9.10	Is the service architected with a minimum of three separate tiers: web services, application, and storage/database?	☐ Yes ☐ No ☐ N/A	Engineering comment required	Vendor Response 9/26. - Yes No response. Question not initially answered by the vendor.
9.11	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	☒ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
	servers, web servers, workstations, the Internet, and other systems by a firewall or restrictive ACLs?			
9.12	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		
9.13	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		
9.14	Does the Vendor actively monitor their cloud/hosted services environment (in real or near real-time) for security incidents?	☒ Yes ☐ No ☐ N/A		
9.15	Does the Vendor have an established security incident management program that complies with legal and regulatory requirements related to incident/breach reporting and notification?	☒ Yes ☐ No ☐ N/A		
9.16	Does the Vendor have dedicated security staff used for responding to security incidents?	☒ Yes ☐ No ☐ N/A		
9.17	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		
9.18	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		
9.19	Will Providence confidential and/or regulated data be accessed or	☒ Yes ☐ No	Confidential data is only visible during a remote session that the customer	

#	Question	Response	Vendor Comments	Providence Comments
	administered by Vendor personnel exclusively within the United States?	☐ **N/A**	must accept from the hospital machine	
9.20	Are information security requirements embedded within the Vendor's Business Continuity and Disaster Recovery Plans and Processes?	☐ **Yes** ☐ **No** ☒ **N/A**	Data is hosted by the customer.	Vendor hosts audit logs and machine data on IntelliMax Enterprise for 30 days, potentially longer. Recommend implementation team ensure BCA and DR plans appropriately support Providence business needs.

10. Cloud Security (IaaS)

Is the Vendor cloud environment an Infrastructure as a Service (IaaS) offering (e.g., AWS, Azure, or GCP)?

(**Note**: Most Vendors should skip this section, unless they are an IaaS hosting provider. Typically, only IaaS providers like Microsoft, Amazon, Google, etc. should complete this section. 3rd Parties that use IaaS services from (Amazon, Microsoft, Google, etc. to operate their own service do not need to complete this section, nor do they need to request that any of these service providers to complete this section. Providence will make a request directly to Amazon, Microsoft, Google, etc. on an as-needed basis if this section applies.

☐ **Yes – Answer the questions below (i.e., if you *are* AWS, Azure, or GCP, select this option and answer the questions below)**

☒ **No – Skip this section and proceed to the next section (i.e., if you *use* AWS, Azure, or GCP to host your online service, then you can skip this section as it is intended only for cloud services providers)**

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

#	Question	Response	Vendor Comments	Providence Comments
10.1	Are file-integrity monitoring tools in place to monitor modifications to critical system files, configuration files, and content files?	☐ **Yes** ☐ **No** ☐ **N/A**		
10.2	Is a formal change management procedure documented and implemented?	☐ **Yes** ☐ **No** ☐ **N/A**		
10.3	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			
10.4	Are vulnerability scans conducted against all internal and external systems and applications at least quarterly and after any significant system changes? (Examples of vulnerability scans include host and application scanning conducted by an industry-standard scanning tool or service like Qualys, Rapid7, or Tenable Nessus.)	☐ Yes ☐ No ☐ N/A		
10.5	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		
10.6	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		
10.7	Are critical, high, and medium risk penetration test findings remediated within a clearly defined and documented timeframe that does not exceed 30 days for critical, high-risk, and Internet-facing medium-risk	☐ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
	vulnerabilities, and 60 days for all other medium-risk vulnerabilities?			
10.8	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		
10.9	Does the Vendor actively monitor their IaaS environment (in real or near real-time) for security incidents?	☐ Yes ☐ No ☐ N/A		
10.10	Does the Vendor have an established security incident management program that complies with legal and regulatory requirements related to incident/breach reporting and notification?	☐ Yes ☐ No ☐ N/A		
10.11	Does the Vendor have dedicated security staff used for responding to security incidents?	☐ Yes ☐ No ☐ N/A		
10.12	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		
10.13	Can Providence use IaaS services from data centers that are geographically located exclusively within the United States?	☐ Yes ☐ No ☐ N/A		
10.14	Will Providence confidential and/or regulated data be accessed or administered by Vendor personnel exclusively within the United States?	☐ Yes ☐ No ☐ N/A		

11. Vendor Datacenter Security

Will Providence data be stored, processed or transmitted within a non-Providence, Vendor datacenter (including a cloud 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
11.1	Does the Vendor encrypt and physically secure all system backup media that contains Providence confidential or regulated data?	☐ Yes ☐ No ☒ N/A		Received update from Elekta via email on 9/12/22. Elekta needs to clarify this with PTC. (Case Opened 16530595) Recommend implementation team to confirm with Elekta that all regulated system backup media is encrypted and physically secure. Elekta documentation states no PHI or confidential information stored or transferred, but this is not the case when IntelliMax connect is utilized. Elekta has required a lot of back and forth questions during the investigation. May be additional risk not disclosed, as information was challenging to obtain.
11.2	Has the Vendor implemented procedures and controls to safeguard its facility and equipment from unauthorized physical access or theft?	☒ Yes ☐ No ☐ N/A		
11.3	Does the Vendor have physical security controls such as card control entry combined with additional biometric or similar multifactor identify validation, access control vestibules (e.g., "mantraps", air locks, or sally ports), security cameras, and uniformed security officers?	☒ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
11.4	Does the Vendor log physical access to facilities that contain Providence confidential and/or regulated data?	☒ Yes ☐ No ☐ N/A		

12. 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
12.1	Has the Vendor implemented a formal asset management program, including inventory of authorized devices and software?	☐ Yes ☐ No ☐ N/A		
12.2	Has the Vendor implemented procedures and controls to safeguard its facility and equipment from unauthorized physical access or theft?	☐ Yes ☐ No ☐ N/A		
12.3	Does the Vendor have a procedure for addressing lost devices such as laptops, cell phones, tablets, etc.?	☐ Yes ☐ No ☐ N/A		
12.4	Does the Vendor have physical security controls such as card control entry, security cameras, and uniformed security officers?	☐ Yes ☐ No ☐ N/A		
12.5	Does the Vendor log physical access to facilities that contain Providence confidential and/or regulated data?	☐ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
12.6	Does the Vendor use Enterprise secure wireless protocols for controlling access to wireless networks?	☐ Yes ☐ No ☐ N/A		
12.7	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		
12.8	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		
12.9	Are workstations and servers protected by host-based anti-malware applications?	☐ Yes ☐ No ☐ N/A		
12.10	Are workstations and servers protected by host-based intrusion detection and protection applications?	☐ Yes ☐ No ☐ N/A		
12.11	Are workstations and servers protected by host-based firewalls?	☐ Yes ☐ No ☐ N/A		
12.12	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		
12.13	Are activities on the corporate network monitored by a Security Operations Center (or equivalent function) that is staffed and equipped with people,	☐ Yes ☐ No ☐ N/A		

#	Question	Response	Vendor Comments	Providence Comments
	processes and technologies to rapidly respond to and remediate information security events?			
12.14	Has the Vendor deployed data-loss prevention technologies that can detect and block attempts to exfiltrate confidential or regulated data?	☐ Yes ☐ No ☐ N/A		
12.15	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		
12.16	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		
12.17	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		
12.18	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		
12.19	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)	☐ 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			
12.20	Does the Vendor conduct vulnerability scans on all internet-facing corporate network assets at least quarterly?	☐ Yes ☐ No ☐ N/A		
12.21	Does the Vendor conduct credentialed/authenticated vulnerability scans on all internal corporate network assets at least quarterly?	☐ Yes ☐ No ☐ N/A		
12.22	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) • <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		
12.23	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		

#	Question	Response	Vendor Comments	Providence Comments
12.24	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		
12.25	Does the Vendor use an email filtering technology to protect its network against phishing, malware, and other email-based attacks?	☐ Yes ☐ No ☐ N/A		
12.26	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		

13. 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
13.1	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		
13.2	Does the Vendor also conduct periodic information security reassessments of	☒ Yes		

#	Question	Response	Vendor Comments	Providence Comments
	Subcontractor solutions or services throughout the duration of the contract with the Subcontractor?	☐ No ☐ N/A		
13.3	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		Received update from Elekta via email on 9/12/22. Elekta Legal team is reviewing Providence comment: Vendor does not agree to use Providence VPN. IntelliMax Agent is intended to cover Elekta remote support.
13.4	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		Received update from Elekta via email on 9/12/22. Elekta Legal team is reviewing Providence comment: Vendor does not agree to use Providence VPN. IntelliMax Agent is intended to cover Elekta remote support.
13.5	Does the Vendor ensure that the Subcontractor signs a Business Associates Agreement (BAA) for Subcontractor solutions or services that will or may store, process, transmit, or access Providence regulated Protected Health Information (PHI)?	☐ Yes ☐ No ☒ N/A		Received update from Elekta via email on 9/12/22. Elekta Legal team is reviewing Providence comment: Elekta documentation states no PHI or confidential information stored or transferred.
13.6	Does the Vendor hold Subcontractors contractually accountable to provide sufficient information security safeguards consistent with the NIST Cybersecurity Framework or other	☐ Yes ☐ No ☒ N/A		Received update from Elekta via email on 9/12/22.

#	Question	Response	Vendor Comments	Providence Comments
	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)?			Elekta Legal team is reviewing Providence comment: No vendor comments from Elekta initially. Elekta documentation states no PHI or confidential information stored or transferred. Elekta Care Support Center (ECSC) employees in the relevant countries that provide support. (These employees can be out of country or out of continent.) File transfer using the remote access client would also make the Elekta IntelliMax support user the recipient of any files. These users are mandated to comply with the storage of any retrieved files in accordance with local Personally Identifiable Data (PID)/ Protected Health Information (PHI) policies.

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: Trevor Worrell	**EIS Analyst Title:** Senior Information Security Analyst
Date Assessed: 9/30/2022	**Peer Reviewer (Optional): Dave Thompson**
Business Stakeholder Ownership and Use Information	
Providence Owner Name: Steve Wimmer	**Providence Contract Manager or Project Manager:** James Harris, Kirsten Halseth
Business Unit: Oncology Services	**Providence C-Level Sponsor:** Ty Walker
Location where the system or service will be used:	☒ **Enterprise (used throughout Providence)** ☐ **Specific Providence Location or Ministry, list all that apply:**

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:		
☒ **Fail**	Providence Enterprise Information Security (EIS) conducted a review of **Elekta IntelliMax Agent / IntelliMax Enterprise Web** 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.	
Observation #	**Observation Description**	**Risk Rating and Tracking**
Observation 1	**Corresponding Question #: 3.1, 3.2** **Finding Description:** Solution does not comply with Providence policy requirements for SSO and MFA. **Risk Description:** IntelliMax Enterprise Web only requires Single Factor Authentication and does not use SSO or MFA. IntelliMax Connect remote support connection with Elekta is initiated onsite by caregiver in Providence hospital on IntelliMax Agent workstation. IntelliMax Agent is locally installed on Providence the workstation with no specific login. Accessing the workstation does require Providence credentials. **Recommendation:** Recommend vendor implement MFA functionality on their public facing website, IntelliMax Enterprise Web.	☐ Very High ☐ High ☒ Moderate ☐ Low ☐ Very Low **Tracked in Risk Register: ☐ Y ☒ N**

	Disposition/Outcome: Vendor response 9/26/22: MFA is not possible with the Axeda solution. We are transitioning to a new infrastructure and MFA will be part of this authentication from the beginning. Axeda capabilities will start to be deprecated from mid 2023.	**Risk Register #:** Click here to enter text.
Observation 2	**Corresponding Question #: 4.4, 4.5, 4.8** **Finding Description:** Access control requirements do not meet Providence policy. Password Management Standard **Risk Description**: IntelliMax Enterprise Web where device data and device status information is sent via IntelliMax Agent uses only username/password for authentication. Vendor solution is unable to configure password re-use requirements, initial reset, or require password length be increased for privileged accounts. **Recommendation:** Recommend vendor improve future iteration of the software to allow for longer password requirements for privileged accounts, configurable password reuse restriction, and add initial password reset requirement. **Disposition/Outcome:** Click here to enter text.	☐ **Very High** ☐ **High** ☒ **Moderate** ☐ **Low** ☐ **Very Low** **Tracked in Risk Register: ☐ Y ☒ N** **Risk Register #:** Click here to enter text.
Observation 3	**Corresponding Question #: Section 5** **Finding Description: TLS less than v1.2, Encryption of data at rest.** Network communications protocols should use encryption, and transmit date using protocols such as TLSv1.2 or above which provide ciphers which align with Providence Cryptographic Protection Standards: https://phs-phs.policystat.com/policy/9850405/latest Disk encryption for data at rest does not meet Providence policy. Elekta does not encrypt devices, but does allow Providence to encrypt workstation. Cryptographic keys are not stored in a secure key vault. **Risk Description:** Vendor noted TLS versions less than TLSv1.2 is used. Unencrypted traffic and unencrypted data at rest exposes data to unauthorized access and unauthorized modification. Vendor required a lot of back and forth questions during the investigation. May be additional risk not disclosed, as information was challenging to obtain. **Recommendation:** Vendor should eliminate use of TLS versions less than TLSv1.2 from the operations of the software. Ensure all infrastructure components which involve network communication use encryption with	☐ **Very High** ☒ **High** ☐ **Moderate** ☐ **Low** ☐ **Very Low** **Tracked in Risk Register: ☐ Y ☒ N** **Risk Register #:** Click here to enter text.

	TLSv1.2 or above. For SSL/TLS traffic, this relates to TLSv1.2. Elekta noted BitLocker should work to encrypt workstations, but has not been vetted by the vendor. Providence IS team verify TLS versions used and work with vendor regarding use of BitLocker encryption. **Disposition/Outcome:** Vendor response 9/26: IntelliMax Agent version 4.2 will use TLSv1.2 or above. This agent version will be rolled out approximately November 2022.	
Observation 4	**Corresponding Question #: 6.3, 6.4, 6.5** **Finding Description:** The Vendor system does not maintain logs that record access to specific records within the application, including which user accessed the record and when. **Risk Description:** Vendor system logs user activity, and transfer of data, but not who viewed a record. **Risk Rationale:** • The Impact is Low because user activity is logged. • The Likelihood is Low because access is limited to specific roles. • The overall Risk Rating is Low because the Impact is Low and the Likelihood is Low. **Recommendation:** Vendor should update logging to include data view to record accessing and view to specific records within the application, including which user accessed the record and when. Providence IS should ensure all applicable logging is enabled for Providence owned devices. Refer to section 6 for additional notes. **Disposition/Outcome:** Click here to enter text.	☐ Very High ☐ High ☐ Moderate ☒ Low ☐ Very Low **Tracked in Risk Register: ☐ Y ☐ N** **Risk Register #:** Click here to enter text.
Observation 5	**Corresponding Question #: 8.1,** **Finding Description:** Vendor does not agree to use Providence provided VPN solution. Elekta IntelliMax includes a remote support connection tool, named IntelliMax Connect. This is not an approved vendor remote access tool. **Risk Description:** VNC is the underlying client/server technology that is used in IntelliMax Connect sessions for remote screen sharing support. VNC is listed on Providence Denied Productivity and Developer Software.	☐ Very High ☒ High ☐ Moderate ☐ Low ☐ Very Low

	Recommendation: Vendor to validate, test, and use the Providence provided VPN solution. **Disposition/Outcome:** **Vendor response 9/26:** Providence VPN is not supported in a standard service contract and would require a non-standard process to be followed that may impact the cost of service/compliance. It is possible to disable IntelliMax Connect. While not formally documented as separate things, IntelliMax Connect can be disabled and the IntelliMax Agent will continue to run. Simply blocking the GAS URLs would also provide this capability. Be aware our Service Agreements mandate the use of IntelliMax Connect to allow us to remotely support products, so other means of remote support will need to be investigated and could impact the service agreement costs.	**Tracked in Risk Register:** ☐ Y ☒ N **Risk Register #:** Click here to enter text.
Observation 6	**Corresponding Question #: 8.2** **Finding Description:** Vendor support may originate from countries outside the US for on-prem device support. **Risk Description:** Vendor access from non-US countries may require additional contract provisions to legally protect Providence should unauthorized data exfiltration occur. **Risk Rationale:** • The Impact is High because the data involved is PHI. • The Likelihood is High because the vendor has indicated that non-US workers may have access to systems which have PHI. • The overall Risk Rating is High because the Impact is High and the Likelihood is High. **Recommendation:** Ensure IT Contracting team comprehends scope of countries which vendor is based. **Disposition/Outcome:** Responsibility for the Providence implementation team to engage IT Contracting as appropriate.	☐ Very High ☒ High ☐ Moderate ☐ Low ☐ Very Low **Tracked in Risk Register:** ☐ Y ☒ N **Risk Register #:** Click here to enter text.
Observation 7	**Corresponding Question #: 8.19, 8.20** **Finding Description:** System hardening is not configured by default. **Risk Description:** VNC is the underlying protocols that is used in IntelliMax Connect sessions for screen sharing. Unnecessary services (ports and protocols) may allow or introduce vulnerabilities to which a network-based attack may leverage to compromise affected systems.	☐ Very High ☐ High ☒ Moderate ☐ Low ☐ Very Low

	Risk Rationale: • The Impact is High because the data involved is PHI. • The Likelihood is Moderate because network access is required to exploit vulnerabilities related to non-essential services. • The overall Risk Rating is Moderate because the Impact is High and the Likelihood is Moderate. **Recommendation**: Recommend implementation team ensure vulnerable protocols are disabled. Unnecessary services should be disabled. Providence team can engage Risk Management or Security Architecture to discuss. **Disposition/Outcome**: Providence implementation team owns the responsibility to ensure only the needed services are configured and enabled.	**Tracked in Risk Register:** ☐ **Y** ☒ **N** **Risk Register #:** Click here to enter text.
Observation 8	**Corresponding Question #: Section 13 – 13.3, 13.4, 13.5, 13.6** **Finding Description**: Downstream third-party vendor or Business Associates may have access to Providence data. Those individuals may not be restricted to United States-based vendor personnel and resources. **Risk Description**: PSJH confidential information shall not be stored or viewed outside of the United States of America (USA) unless approved by PSJH Legal, and there shall be an offshore agreement or other relevant or mandated documentation in place as part of the contract or agreement. **Risk Rationale**: • The Impact is High because vulnerabilities executed remotely may allow unauthorized users from unknown locations the ability to damage network systems or exfiltrate configuration sets for future attacks. • The Likelihood is Moderate because exploitation requires an existing vulnerability in combination within a timeframe which an attacker can take advantage. • The overall Risk Rating is Moderate because the Impact is High and the Likelihood is Moderate. **Recommendation**: Recommend Providence Legal and contracting team ensure vendor BAA, MSA meets Providence requirements in regards to location of vendor personnel who may need access to Providence data. **Disposition/Outcome**: Providence implementation team owns the responsibility to ensure IT Contracting team reviews to determine the applicability of this finding.	☐ **Very High** ☐ **High** ☒ **Moderate** ☐ **Low** ☐ **Very Low** **Tracked in Risk Register:** ☐ **Y** ☒ **N** **Risk Register #:** Click here to enter text.

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.