Ascension Technologies: Technology Assessment Vendor Questionnaire Application

1. Please answer ALL questions in and provide enough detail to properly address the question.
2. If you answer "No" or "NA," an explanation must be provided in the comments section stating why this requirement is either not met or not relevant.
3. Attach the diagrams separately, DO NOT EMBED any documents into this questionnaire.
4. Required Documents will include, but are not limited to:
--- Architecture Diagram
--- Data Flow Diagram
--- A FULL SOC 2 Type II or HITRUST, if the product is cloud-based or vendor hosted. Further Instruction can be found in the Cloud section.

Failure to follow these guidelines will result in a rejection of the Tech Assessment.

	Vendor Information					
CONTACTS	Vendor Company Name			Product Name		
	Contact Name (Person Completing form):		Date Completed			
	Product Expert Contact Name:		Phone Number		Email	
	Technical Expert Contact Name:		Phone Number		Email	
	Name of Ascension employee with which you are working:		Phone Number		Email	

	General Questions	Vendor Response
General	**1.** Please provide a **detailed** Application Overview. Explain the purpose of this product and how it is used.	
	2. Is this an On-premise solution, cloud solution, or both? For on-premise, please list equipment types (Servers, etc.):	
	3. Provide Security at Rest and in motion details:	
	4. Are you aware of any other Ascension Facilities that have implemented this product? If so, please provide locations.	

	Security Questions	Select Answer	Comments
SECURITY	**5.** Will the solution create, modify, store or transmit Ascension electronic PHI, PII or PCI information? *Definition of PHI & PII are provided on at the end of this document.* Select the appropriate drop down.	...	
	6. Unique identifiers is an Ascension standard. Is your solution able to implement unique identifiers for all accesses by users, vendors, administrators, support staff, processes, or interfaces which access or manipulate data?	...	
	7. Does your solution utilize encryption or hashing to protect passwords?	...	
	8. Does your solution have the capability of logging all application access, including: view, change, add and delete?	...	
	9. Is the solution able to retain application access logs for 12 months that can be made available for Ascension review?	...	
	10. Is access to this solution role based?	...	
	11. Are all data transmissions across open or public networks encrypted?	...	
	12. Does this solution provide for prompt notification to Ascension in the event of a security incident that would put Ascension data at risk of exposure to an unauthorized entity/person?	...	
	13. If your solution/application/process requires remote access into the Ascension environment, are you able to use the Ascension Securelink solution? If answer is "No" then please provide reason(s) in the comments section.	...	
	14. Does your solution contain controls to protect data or information to ensure that it has not been altered or destroyed in an unauthorized manner?	...	
	15. Does this solution support TLS 1.2 or later? Please list latest ?	...	

	Infrastructure Questions	Select Answer	Comments
INFRASTRUCTURE	**16.** Ascension Technologies standard supported server OS is Windows 2016 or later & Linux OS is RHEL 7 or later. Is the solution compatible with either applicable platforms **(On-Premise solutions)**?	...	
	17. Does your solution implement latest O/S platform patching and/or updates (On-Premise solution)?	...	
	18. Will all patches be applied as they are released (On-Premise solution)?	...	
	19. Does your application support Windows 10 (On-Premise solutions that may implement Fat clients)?	...	
	20. If the system requires use of any database technology, which brand of database technology would that be (On-Premise solution)?	...	
	21. What is the latest version of the database that is certified for use by the application (On-Premise solution)?	...	
	22. Will Ascension DBA resources be accountable for any aspect of support on the SQL solution (On premise solution)?	...	
	23. Can a vulnerability binary scan report be provided for your solution (On-premise solution)?	...	
	24. Does your solution implement wireless devices (mobile devices, etc.) and if so, explain (IE: Bluetooth, WIFI, etc.)?	...	
DISASTER RECOVERY	Disaster Recovery Questions	Select Answer	Comments
	25. Do you have specific data backup processes, procedures or tools that have to be used? (For example: do you perform database backups to disk that Ascension can backup using our standard backup process? If yes, please provide details in the comments section.)	...	
	26. Do you have a contracted recovery / resiliency strategy?. If yes, attach to this document.	...	
	27. Do you have a contracted threshold for maximum data loss or projected recovery time? If yes, list thresholds in the comments section.	...	

If the solution is cloud based, please answer additional questions below. Questions in this section are concerning the **application vendor**, not 3rd-party providers or subcontractors.

Ascension requires the current, full SOC 2 Type 2 or HITRUST report for all cloud-based or vendor hosted solutions so we can review the internal security controls of third parties accessing, processing, or storing Ascension ePHI or PII. This is not negotiable, it's a contractual requirement included in our master contract, and outlined in Ascension's Information Security and Third Party Security Requirements policies. As an alternative, if the vendor will contractually commit to obtaining a SOC 2 Type II or HITRUST within 12 months of signing, we can approve the TA with that condition.

The Completion date of the current full SOC 2 Type 2 or HITRUST report must be added to the appropriate box. The date is used to determine the validity of the report. For example, if the report ran from January 1, 2020 through Dec 31, 2020, the ending date would be calculated from Dec 31, 2020.
- In general, if the report is for a 6 month time period, if it is older than 9 months from the ending date of the audit period, we will request a new report.
- For a 12 month report, if it is older than 15 months, we will request a new report

A SOC 2 Type 2 report or HITRUST certification is required when:
1. a solution is submitted to the Technology Assessment process that requires an Ascension Associate's login to a third-party web or hosted site to obtain information or perform a function if the Associate uses Public PII and Sensitive PII,
2. a solution is submitted to the Technology Assessment process that requires data containing Ascension Associate's Public and Sensitive PII be transmitted outside of the Ascension network.

A SOC 2 Type 2 report or HITRUST certification is not required when:
1. a solution is submitted to the Technology Assessment process that requires an Ascension Associate's login to a third-party web or hosted site to obtain information or perform a function if the Associate uses only Public PII such as their First and Last name, Ascension email address and/or an Ascension telephone number
2. a solution is submitted to the Technology Assessment process which requires that data containing only Ascension Associate's Public PII be transmitted outside of the Ascension network

	Vendor Security Question	Select Answer	Comments
Vendor Security	**28.** Can your organization provide periodic and contiguous SOC 2 Type 2 audits and/or HITRUST certifications to Ascension? Please include certification/audit documents when submitting this form. SOC 2 Type II forms must be no more than 15 months and HITRUST no more than 24 months past the ending date of the evaluation. **Attach at the time of submission.**	...	
	28a. Enter Completion date of Current SOC2 or HITRUST		
	29. If you do not have a current full SOC2 Type II or HiTRUST, are you willing to contractually commit to obtaining one in the next 12 months .	...	
	30. Will supplier store, access, transmit and/or process Ascension ePHI, personally identifiable information (PII), or other sensitive data outside of the United States?	...	
	31. Does your organization periodically perform a security risk assessment on your solution?	...	
	32. What are the location(s) from which Ascension data will be stored and/or accessed?		

If your cloud-based solution uses any subcontractors or 3rd party providers, please complete the following section for each individual provider.				
Note: Ascension keeps current copies of SOC2 Type II certifications for Amazon Web Services, Google and Microsoft Web Services so it is not necessary to submit certifications for these organizations. If one of these suppliers is a subcontractor for your product, please acknowledge on this form.				
	Subcontractor #1 Name:		Select Answer	Comments
Subcontractor 1	**33.** Please provide current full SOC-2 Type 2 audit or HITRUST certification to Ascension for your hosting subcontractor. Include certification/audit documents when submitting this form. SOC 2 Type II forms must be no more than 15 months and HITRUST no more than 24 months past the ending date of the evaluation. **Attach at the time of submission.**		...	
	33a. Enter Completion date of Current SOC2 or HITRUST			
	34. If your hosting provider does not have a current SOC2 Type II ot HiTRUST, are you in discussion with the hosting provider to obtain one?		...	
	35. Will supplier store, access, transmit and/or process Ascension ePHI, personally identifiable information (PII), or other sensitive data outside of the United States?		...	
	36. Does the host provider periodically perform a security risk assessment?		...	
	37. What are the location(s) from which Ascension data will be stored and/or accessed?			

	Subcontractor #2 Name:		Select Answer	Vendor Comments
SUBCONTRACTOR 2	**38**. Please provide current full SOC-2 Type 2 audit or HITRUST certification to Ascension for your hosting subcontractor. Include certification/audit documents when submitting this form. SOC 2 Type II forms must be no more than 15 months and HITRUST no more than 24 months past the ending date of the evaluation. **Attach at the time of submission.**		...	
	38a. Enter Completion date of Current SOC2 or HITRUST			
	39. If your hosting provider does not have a current SOC2 Type II ot HiTRUST, are you in discussion with the hosting provider to obtain one?		...	
	40. Will supplier store, access, transmit and/or process Ascension ePHI, personally identifiable information (PII), or other sensitive data outside of the United States?		...	
	41. Does the host provider periodically perform a security risk assessment?		...	
	42. What are the location(s) from which Ascension data will be stored and/or accessed?			

	Subcontractor #3 Name:					Select Answer	Vendor Comments			
SUBCONTRACTOR 3	**43**. Please provide current full SOC-2 Type 2 audit or HITRUST certification to Ascension for your hosting subcontractor. Include certification/audit documents when submitting this form. SOC 2 Type II forms must be no more than 15 months and HITRUST no more than 24 months past the ending date of the evaluation. **Attach at the time of submission.**					...				
	43a. Enter Completion date of Current SOC2 or HITRUST									
	44. If your hosting provider does not have a current SOC2 Type II ot HiTRUST, are you in discussion with the hosting provider to obtain one?					...				
	45. Will supplier store, access, transmit and/or process Ascension ePHI, personally identifiable information (PII), or other sensitive data outside of the United States?					...				
	46. Does the host provider periodically perform a security risk assessment?					...				
	47. What are the location(s) from which Ascension data will be stored and/or accessed?					...				