TEMPLATE INSTRUCTIONS AND NOTES (DELETE BEFORE PUBLISHING)

- The following includes a list of suggested questions to collect from any potential third-party that may serve as a Business Associate and collect, view, transmit, or store ePHI or other sensitive information on behalf of the organization. The Assessment is ideally completed during procurement to inform contract negotiations and future management.
- Given the resource effort required to evaluate third-parties, Online recommends organizations conduct assessments on any vendor that may be deemed a Business Associate.
- The Assessment Questionnaire should be accompanied with a scoring mechanism to assess vendor scores.
- Results of the assessment questionnaire should serve as an input to a vendor risk assessment which should be done prior to sharing ePHI with a vendor.

Third-Party Vendor Security Assessment Questionnaire

Vendor Name	
Assessment Date	
Vendor Point of Contact	

#	Question	Response	Notes or Considerations
Information Security			
1.	Does your organization maintain a security program?		
2.	Please provide the designated Security Official for your organization.		
3.	Do you have a recent third-party attestations that can be provided to support the assessment?		Examples include HITRUST certification, SOC-2 Report, ISO 27001: 2013, or a third-party assessment against a recognized security standard)

#	Question	Response	Notes or Considerations
4.	Does your organization have documented security and privacy policies?		
5.	Do you conduct regular risk assessments? If so, provide the date of last risk assessment.		
Data Access and Storage			
6.	What type of <organization> data do you anticipate accessing as part of this contract?		
7.	How is <organization> data stored (if applicable)?		
8.	How often is <organization> data backed up?		
9.	Do you have a Business Continuity and Disaster Recovery Plan?		
10.	Is data encrypted at rest and in transit (as applicable)?		
11.	Do you support Role-Based Access Controls?		
12.	Do you support Single Sign On or Federated Identify Management?		
13.	Do you support MFA?		
14.	Does your system include shared or generic accounts? (if applicable)?		
15.	Do you have any staff accessing <organization> data outside of continental US?		
Workforce Security			
16.	Do you conduct background checks on employees?		
17.	Are employees required to complete annual Security Training?		
18.	Do you contract with any subcontractors who might view, access, transmit, or		

#	Question	Response	Notes or Considerations
	store <organization> data on your behalf? If so, how do those vendors access data?		
Other			
19.	Do you have an Incident Response Plan?		
20.	How are patches and vulnerabilities managed within the environment?		
21.	Does your organization perform regular penetration tests?		
22.	Is there any other information your organization wishes to share as it relates to the security of <organization> data?		
23.	Has your organization experienced a breach in the past two years?		

Revision History

Version	Date	Author	Description of Change	Approvers
0.01	7/25/23	M.Erikson	Initial draft	