How to Choose a Third-Party Vendor

For practices that choose to engage third-party cybersecurity vendors and IT professionals (such as managed service providers, or MSPs), thorough vetting of their offerings is necessary. While many organizations may claim to be "HIPAA- and HITECH-compliant," this is not a formal designation, and critical assessment is paramount. While many "all-in-one" IT providers or internal experts are excellent for general updates and IT services, it's important to engage cybersecurity specialists with a comprehensive understanding of security processes and programs. Below is a list of questions that will help you better understand the qualifications and security measures a third-party organization or individual contractor can offer your practice. Their responses can be used during this selection process to help guide decision-making to choose the most knowledgeable and secure partner.

1. Is your security program based on a publicly vetted framework? (NIST, CIS, Cloud Security Alliance)
2. What is the maturity level of your organization related to the framework you are using?
3. Do you have a designated information security officer or similar role within your organization?
4. How many security professionals are in your organization?
5. Do the security professionals hold any certifications? (CISSP, CISM, CCSP, etc.)
6. Can you provide a copy of your security plan and policies? (If they are unable or unwilling to share, ask for a copy of the table of content for those documents.)
7. How does your organization support compliance requirements for customers? (PCI, CMMC, HIPAA)
8. Do you use subcontractors to deliver any of the IT and security services for customers?
9. What type of background checks are performed on employees and contractors?
10. What security technology do you currently employ for internal infrastructure?
11. How do you manage risk?
12. Where do you store client data?
13. Do you conduct regular vulnerability scans?
14. How do you conduct asset management?

15. How do you manage configuration changes to its internal systems?
16. How do you access the client environment?
17. Is the infrastructure used to support customers hosted on premises or in the cloud?
18. What controls do you have in place to prevent lateral movement of an attacker?
19. Do you have a process for managing privileged accounts?
20. What is your policy on log retention?
21. Do you operate a security operations center or subscribe to a third party for the service?
22. Does your organization have defined and documented backup and recovery strategies for systems that contain client data?
23. Does your organization undergo annual testing of security controls by a third party?
24. Do you have a detailed and documented incident response plan?
25. Does the customer have the right to audit?
26. Do you have cybersecurity insurance coverage?

This document was developed in part with expert insight from our partners at Sentinel Risk Advisors and Tokio Marine America.

Curi is pleased to provide you with this content, and we hope that you find it useful. Though we have found that the use of such information may help reduce cyber risks medical practices face, Curi cannot guarantee that using this or any other information/service/tool will prevent a claim against, or security incident/breach/investigation/fine/penalty involving, you or your practice. Curi cannot and does not offer legal advice. If you or your practice requires legal advice, please contact independent counsel. If you have further questions, please feel free to contact our office.