

# Vendor Cybersecurity & HIPAA Due-Diligence Questionnaire

Please answer these 12 questions for the service/product listed below. You can attach or link to existing documentation instead of repeating it. If a question does not apply, write N/A and briefly explain why it does not apply.

|                       |  |
|-----------------------|--|
| Practice/Organization |  |
| Vendor                |  |
| Service/Product       |  |
| Vendor Contact        |  |
| Date Completed        |  |

## 1. What information and access will you need - and why?

### Please include:

- What information you will create, receive, store, send, or access, including protected health information (PHI) or other sensitive information.
- What access you need to our systems, network, devices, accounts, integrations, or remote-support tools.
- Why each type of access is needed and where our information will be stored or processed.

|  |
|--|
|  |
|--|

## 2. If a BAA is required, will you sign one? Do any other companies you use have access to our patient information?

### Please include:

- Whether you will sign an appropriate Business Associate Agreement (BAA) before handling PHI when one is required.
- Any subcontractors or other companies that may handle our PHI while helping you provide this service.
- How the applicable privacy and security requirements are passed to those companies.

|  |
|--|
|  |
|--|

### 3. How do you control who can access our data and systems?

**Please include:**

- How access is approved, reviewed, changed, and removed, including unique accounts and access based on job need.
- Where you require multifactor authentication (MFA), including remote access, internet-facing systems, administrator access, and other high-risk access.
- How administrator and service accounts are controlled

### 4. How do you protect the computers, servers, and other systems that store or access our information?

**Please include:**

- How relevant systems are kept supported, updated, securely configured, and protected from malicious or suspicious activity.
- How sensitive information is protected while it is being sent, while it is stored, and in backups.
- Any important exceptions, why they exist, and the safeguards you use instead.

### 5. How do you find and fix security weaknesses - including problems with older or connected medical devices?

**Please include:**

- How you keep track of the systems and devices used to provide the service, find security weaknesses, decide what to fix first, and verify security updates.
- How you handle technology that cannot be patched or replaced quickly.
- For older or connected medical devices, any isolation, access limits, monitoring, remote-access controls, and replacement plans.

## 6. How do you protect your team from phishing, social engineering, and human error?

### **Please include:**

- Your recurring security-awareness training and any additional training for higher-risk roles.
- Email and phishing protections.
- How team members report suspicious messages or activity, and what technical protections are in place when someone does click or respond to a phishing attempt.

## 7. How do you detect suspicious activity and figure out what happened?

### **Please include:**

- What important security activities you record and monitor, how long those records are kept, and what parts of the service this covers.
- How concerns are escalated and investigated.
- Whether you can determine who accessed sensitive systems, what changed, and what information may have been affected.

## 8. If there is a security incident, how will you respond - and when will you tell us?

### **Please include:**

- How you contain, investigate, recover from, and communicate about a security incident, including who will communicate with us and whether your notification commitment is in the contract.
- How often you test your incident-response process.
- How quickly you will notify us after discovering an incident that materially affects our data or service, and what event starts that time period.

## 9. If your systems fail or are attacked, how will you keep our practice operating and restore our data or service?

### **Please include:**

- How backups are protected and how recovery is tested, including the date of the most recent successful restore or recovery test relevant to this service, and how problems found during testing are tracked and corrected.
  - How quickly critical services are expected to return and how much recent data could be lost.
  - Any continuity or failover options and important outside services or companies that could slow recovery.
- 

## 10. What evidence can you provide that your security program is actually working?

### **Please include:**

- Current evidence appropriate to this service. Examples may include security testing, risk assessments, restore-test results, independent assessments, audit reports, certifications, or comparable evidence.
  - The date and scope of the evidence and what parts of this service it covers, what it does not cover, and how significant findings have been resolved and which are still being addressed.
  - You may attach or link to existing documents instead of repeating them here.
- 

## 11. Will any of our information be processed by artificial intelligence or used to train or improve an AI system?

### **Please include:**

- Whether this service uses artificial intelligence (AI) with our information and, if so, the AI system or provider, any other companies involved, and why it is used.
  - What information the AI receives, how long it is kept, and whether it is used to train, fine-tune, test, or improve AI models or services.
  - How PHI is handled under the applicable HIPAA relationship.
-

## 12. Who is responsible for security, and what happens to our data and access when the relationship changes or ends?

**Please include:**

- Which important security responsibilities belong to you, which belong to us, and which are shared, and when those responsibilities are reviewed.
- How we can export our data and how data will be returned, retained, or destroyed.
- How accounts, integrations, remote access, and other access will be removed, and what transition help you provide.