Wellness Agent AI: Vendor Inventory & BAA Status

Complete Vendor Management for HIPAA Compliance

Status: COMPLIANCE READY
Version: 1.0.0
Date: 2025-01-XX
Pattern: VENDOR × MANAGEMENT × HIPAA × BAA × ONE

EXECUTIVE SUMMARY

This document tracks all vendors that may access, process, or store PHI/ePHI in Wellness Agent AI. For each vendor, we document:

- **PHI Access Level:** What PHI they can access
- **HIPAA-Eligible Status:** Whether they offer HIPAA-eligible services
- **BAA Status:** Whether we have a signed BAA
- **Risk Level:** High/Medium/Low based on PHI access
- **Alternatives:** Backup vendors if BAA unavailable

VENDOR INVENTORY TEMPLATE

How to Use This Template

For each vendor, complete:

1. **Vendor Information:** Name, service type, contact
2. **PHI Access Assessment:** What PHI they can access
3. **HIPAA Eligibility:** Check their HIPAA-eligible offerings
4. **BAA Status:** Track BAA execution
5. **Risk Assessment:** Evaluate risk level
6. **Mitigation:** Controls to reduce risk

TIER 1: CRITICAL VENDORS (Must Have BAAs)

1. Cloud Infrastructure Provider

Option A: Amazon Web Services (AWS)

Vendor Information:

- **Name:** Amazon Web Services, Inc.
- **Service Type:** Cloud Infrastructure (Compute, Storage, Database, Networking)
- **Contact:** aws-hipaa@amazon.com
- **Website:** https://aws.amazon.com/compliance/hipaa-compliance/

PHI Access Level: **HIGH**

- Hosts all infrastructure
- Can access all ePHI at rest and in transit
- Database backups, logs, snapshots

HIPAA-Eligible Services:

- EC2, S3, RDS, Lambda, API Gateway, CloudWatch, etc.
- Most AWS services are HIPAA-eligible
- AWS Business Associate Addendum (BAA) available

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]
- [ ] **BAA Expires:** [Date]
- [ ] **BAA Location:** [File path/URL]

Risk Level: **HIGH**

- Hosts all PHI
- Critical infrastructure dependency

Mitigation:

- Encryption at rest (S3, RDS, EBS)
- Encryption in transit (TLS)
- IAM access controls
- CloudTrail audit logging
- VPC network isolation

Alternatives:

- Microsoft Azure (HIPAA-eligible)
- Google Cloud Platform (HIPAA-eligible)

Option B: Microsoft Azure

Vendor Information:

- **Name:** Microsoft Corporation
- **Service Type:** Cloud Infrastructure
- **Contact:** azurecompliance@microsoft.com
- **Website:** https://azure.microsoft.com/en-us/support/legal/hipaa/

PHI Access Level: **HIGH**

- Hosts all infrastructure
- Can access all ePHI

HIPAA-Eligible Services:

- Azure Compute, Storage, Database, Networking

- Azure BAA available

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **HIGH**

Alternatives:

- AWS (HIPAA-eligible)
- Google Cloud Platform (HIPAA-eligible)

Option C: Google Cloud Platform (GCP)

Vendor Information:

- **Name:** Google LLC
- **Service Type:** Cloud Infrastructure
- **Contact:** gcp-compliance@google.com
- **Website:** https://cloud.google.com/security/compliance/hipaa

PHI Access Level: **HIGH**

HIPAA-Eligible Services:

- GCP Compute, Storage, Database services
- GCP BAA available

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **HIGH**

---

2. LLM Provider

Option A: OpenAI

Vendor Information:

- **Name:** OpenAI, L.L.C.
- **Service Type:** Large Language Model API (GPT-4, GPT-3.5)
- **Contact:** enterprise@openai.com
- **Website:** https://openai.com/enterprise-privacy

PHI Access Level: **HIGH**

- Receives PHI in prompts
- Can see conversation context

- May cache prompts/responses

HIPAA-Eligible Services:

- ⚠ **Check:** OpenAI Enterprise may offer HIPAA-eligible services
- ⚠ **Verify:** BAA availability for enterprise customers
- ⚠ **Note:** Standard API may not be HIPAA-eligible

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]
- [ ] **No Training Clause:** Confirmed in BAA

Risk Level: **HIGH**

- PHI leaves your infrastructure
- High compliance risk

Mitigation:

- Minimum necessary PHI in prompts
- Pseudonymization where possible
- No training on your data (contractual)
- Audit logging of all API calls
- Consider self-hosted alternative for high-security deployments

Alternatives:

- Anthropic Claude (check BAA availability)
- Self-hosted LLM (Llama, Mistral, etc.)
- Azure OpenAI (may have better HIPAA support)

Option B: Anthropic

Vendor Information:

- **Name:** Anthropic PBC
- **Service Type:** Large Language Model API (Claude)
- **Contact:** enterprise@anthropic.com
- **Website:** https://www.anthropic.com/compliance

PHI Access Level: **HIGH**

HIPAA-Eligible Services:

- ⚠ **Check:** Enterprise offerings may include HIPAA support
- ⚠ **Verify:** BAA availability

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **HIGH**

Alternatives:

- OpenAI Enterprise
- Self-hosted LLM
- Azure OpenAI

Option C: Self-Hosted LLM

Vendor Information:

- **Name:** Self-Hosted (Llama, Mistral, etc.)
- **Service Type:** On-premises or self-managed LLM
- **Contact:** N/A

PHI Access Level: **MEDIUM**

- PHI stays in your infrastructure
- You control all security

HIPAA-Eligible Services:

- N/A (you're the BA, not a vendor)

BAA Status:

- **N/A** (no vendor, you're responsible)

Risk Level: **MEDIUM**

- Lower compliance risk (no vendor)
- Higher infrastructure responsibility

Mitigation:

- All Security Rule controls apply
- Encryption, access controls, audit logs
- Model security hardening

---

3. Vector Database

Option A: Pinecone

Vendor Information:

- **Name:** Pinecone Systems, Inc.
- **Service Type:** Managed Vector Database
- **Contact:** support@pinecone.io
- **Website:** https://www.pinecone.io/security-compliance/

PHI Access Level: **HIGH**

- Stores embeddings created from PHI
- Embeddings are ePHI (reversible)

HIPAA-Eligible Services:

- ⚠ **Check:** Enterprise plan may offer HIPAA support
- ⚠ **Verify:** BAA availability

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **HIGH**

- Embeddings contain PHI signal

Mitigation:

- Per-tenant indexes
- Row-level access controls
- Encryption at rest
- Audit logging

Alternatives:

- Weaviate (self-hosted or cloud, check BAA)
- Self-hosted vector DB (Qdrant, Milvus)
- AWS OpenSearch (HIPAA-eligible with BAA)

Option B: Weaviate

Vendor Information:

- **Name:** Weaviate B.V.
- **Service Type:** Vector Database (self-hosted or cloud)
- **Contact:** support@weaviate.io

PHI Access Level: **HIGH** (if cloud) / **MEDIUM** (if self-hosted)

HIPAA-Eligible Services:

- ⚠ **Check:** Cloud offering BAA availability
- Self-hosted: N/A (you're responsible)

BAA Status:

- [ ] **BAA Requested:** [Date] (if cloud)
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **HIGH** (cloud) / **MEDIUM** (self-hosted)

Alternatives:

- Pinecone
- Self-hosted Qdrant/Milvus
- AWS OpenSearch

4. Database Provider

Option A: AWS RDS (PostgreSQL/MySQL)

Vendor Information:

- **Name:** Amazon Web Services (RDS)
- **Service Type:** Managed Relational Database
- **Contact:** Included in AWS BAA

PHI Access Level: HIGH

- Stores all PHI in database

HIPAA-Eligible Services:

- RDS is HIPAA-eligible
- Covered under AWS BAA

BAA Status:

- **Covered under AWS BAA**

Risk Level: HIGH

Mitigation:

- Encryption at rest
- Encryption in transit
- Automated backups (encrypted)
- Database access controls

Option B: MongoDB Atlas

Vendor Information:

- **Name:** MongoDB, Inc.
- **Service Type:** Managed NoSQL Database
- **Contact:** enterprise@mongodb.com

PHI Access Level: HIGH

HIPAA-Eligible Services:

- ⚠ **Check:** Enterprise plan HIPAA support
- ⚠ **Verify:** BAA availability

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: HIGH

Alternatives:

- AWS DocumentDB (covered under AWS BAA)
- Self-hosted MongoDB

---

5. EHR Integration Vendor

Epic Systems

Vendor Information:

- **Name:** Epic Systems Corporation
- **Service Type:** EHR Integration (FHIR/HL7)
- **Contact:** [Customer-specific]

PHI Access Level: **HIGH**

- Full PHI exchange via FHIR/HL7

HIPAA-Eligible Services:

- Epic is a Covered Entity
- Standard BAA for integrations

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **HIGH**

Alternatives:

- Cerner (now Oracle Health)
- Allscripts
- Other EHR vendors

---

6. Messaging Provider

Option A: SendGrid (Twilio)

Vendor Information:

- **Name:** Twilio SendGrid, Inc.
- **Service Type:** Email Service Provider
- **Contact:** support@sendgrid.com

PHI Access Level: **MEDIUM**

- Email messages may contain PHI
- Email content visible to provider

HIPAA-Eligible Services:

- ⚠ **Check:** Enterprise plan HIPAA support
- ⚠ **Verify:** BAA availability

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **MEDIUM**

Mitigation:

- Encrypt email content
- Avoid PHI in subject lines
- Use secure messaging for PHI

Alternatives:

- AWS SES (covered under AWS BAA)
- Microsoft 365 (if using Azure)
- Self-hosted email server

Option B: Twilio (SMS)

Vendor Information:

- **Name:** Twilio, Inc.
- **Service Type:** SMS/Text Messaging
- **Contact:** support@twilio.com

PHI Access Level: **MEDIUM**

- SMS messages may contain PHI

HIPAA-Eligible Services:

- ⚠ **Check:** Enterprise plan HIPAA support
- ⚠ **Verify:** BAA availability

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **MEDIUM**

Mitigation:

- Avoid PHI in SMS when possible
- Use secure messaging app for PHI
- Encrypt SMS content

Alternatives:

- AWS SNS (covered under AWS BAA)
- Self-hosted SMS gateway

TIER 2: SECONDARY VENDORS (BAA If PHI Present)

7. Logging Platform

Option A: Datadog

Vendor Information:

- **Name:** Datadog, Inc.
- **Service Type:** Application Monitoring & Logging
- **Contact:** enterprise@datadog.com

PHI Access Level: MEDIUM

- Logs may contain PHI if not masked
- Error traces may contain PHI

HIPAA-Eligible Services:

- ⚠ **Check:** Enterprise plan HIPAA support
- ⚠ **Verify:** BAA availability

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: MEDIUM

Mitigation:

- Mask/strip PHI in logs
- Pseudonymize identifiers
- Separate PHI logs from non-PHI logs

Alternatives:

- AWS CloudWatch (covered under AWS BAA)
- Self-hosted ELK stack
- Splunk (check BAA availability)

Option B: AWS CloudWatch

Vendor Information:

- **Name:** Amazon Web Services (CloudWatch)
- **Service Type:** Logging & Monitoring
- **Contact:** Covered under AWS BAA

PHI Access Level: MEDIUM

HIPAA-Eligible Services:

- Covered under AWS BAA

BAA Status:

- **Covered under AWS BAA**

Risk Level: **MEDIUM**

Mitigation:

- Mask PHI in logs
- Use log filters to exclude PHI

---

8. Authentication Provider

Option A: Auth0

Vendor Information:

- **Name:** Auth0, Inc. (now Okta)
- **Service Type:** Authentication & Authorization
- **Contact:** enterprise@auth0.com

PHI Access Level: **LOW**

- User identifiers (email, name)
- Not health information itself

HIPAA-Eligible Services:

- ⚠ **Check:** Enterprise plan HIPAA support
- ⚠ **Verify:** BAA availability

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **LOW-MEDIUM**

Mitigation:

- User identifiers are minimal PHI
- MFA enabled
- Access controls

Alternatives:

- AWS Cognito (covered under AWS BAA)
- Self-hosted authentication

Option B: AWS Cognito

Vendor Information:

- **Name:** Amazon Web Services (Cognito)
- **Service Type:** Authentication & User Management
- **Contact:** Covered under AWS BAA

PHI Access Level: **LOW**

HIPAA-Eligible Services:

- Covered under AWS BAA

BAA Status:

- **Covered under AWS BAA**

Risk Level: **LOW**

---

9. Error Tracking

Option A: Sentry

Vendor Information:

- **Name:** Sentry, Inc.
- **Service Type:** Error Tracking & Monitoring
- **Contact:** enterprise@sentry.io

PHI Access Level: **MEDIUM**

- Error traces may contain PHI
- Stack traces may include PHI in variables

HIPAA-Eligible Services:

- ⚠ **Check:** Enterprise plan HIPAA support
- ⚠ **Verify:** BAA availability

BAA Status:

- [ ] **BAA Requested:** [Date]
- [ ] **BAA Received:** [Date]
- [ ] **BAA Executed:** [Date]

Risk Level: **MEDIUM**

Mitigation:

- Sanitize error traces
- Remove PHI from stack traces
- Use data scrubbing

Alternatives:

- Self-hosted Sentry
- AWS X-Ray (covered under AWS BAA)

- Rollbar (check BAA availability)

---

10. Analytics Platform

Option A: Self-Hosted Analytics (PostHog)

Vendor Information:

- **Name:** Self-Hosted PostHog
- **Service Type:** Product Analytics
- **Contact:** N/A

PHI Access Level: **LOW**

- Pseudonymized analytics only
- No PHI in analytics

HIPAA-Eligible Services:

- N/A (you're responsible)

BAA Status:

- **N/A** (no vendor)

Risk Level: **LOW**

Mitigation:

- Pseudonymize all identifiers
- No PHI in analytics events
- Separate from PHI logs

Option B: AWS Analytics Services

Vendor Information:

- **Name:** Amazon Web Services (Kinesis, Redshift, etc.)
- **Service Type:** Analytics & Data Warehousing
- **Contact:** Covered under AWS BAA

PHI Access Level: **MEDIUM** (if PHI present)

HIPAA-Eligible Services:

- Covered under AWS BAA

BAA Status:

- **Covered under AWS BAA**

Risk Level: **MEDIUM**

Mitigation:

- Use only for de-identified analytics
- Or ensure proper encryption/controls

TIER 3: VENDORS TO AVOID (No BAA Available)

Ad Networks & Marketing Analytics

Vendors to Avoid:

- Google Analytics (standard) - No BAA, don't send PHI
- Facebook Pixel - No BAA, don't send PHI
- Marketing automation tools (unless HIPAA-eligible)

Mitigation:

- Use only for non-PHI marketing pages
- Disable on health-context pages
- Use HIPAA-eligible alternatives for PHI analytics

VENDOR RISK ASSESSMENT MATRIX

Vendor	PHI Access	BAA Status	Risk Level	Priority
Cloud Provider (AWS/Azure/GCP)	High	Required	High	P0
LLM Provider	High	⚠ Check	High	P0
Vector Database	High	⚠ Check	High	P0
Database Provider	High	Required	High	P0
EHR Integration	High	Required	High	P0
Messaging (Email/SMS)	Medium	⚠ Check	Medium	P1
Logging Platform	Medium	⚠ Check	Medium	P1
Authentication	Low	⚠ Check	Low	P2
Error Tracking	Medium	⚠ Check	Medium	P1
Analytics	Low/None	Self-hosted	Low	P2

BAA EXECUTION CHECKLIST

For each vendor requiring a BAA:

- [ ] **Identify vendor contact** for BAA requests
- [ ] **Request BAA** (email template below)
- [ ] **Review BAA terms** (legal review recommended)
- [ ] **Negotiate terms** if needed (no training on PHI, etc.)
- [ ] **Execute BAA** (signature from authorized representative)
- [ ] **Store BAA** (secure location, version control)
- [ ] **Track expiration** (renew before expiration)
- [ ] **Update vendor inventory** (mark as complete)

BAA Request Email Template

```
Subject: Business Associate Agreement Request - [Your Company Name]

Dear [Vendor Name] HIPAA Compliance Team,

We are implementing Wellness Agent AI, a healthcare AI platform that will process Protected Health
Information (PHI) on behalf of Covered Entities.

We require a Business Associate Agreement (BAA) for your [Service Name] service as part of our HIPAA
compliance program.

Please provide:
1. Your standard BAA template
2. Instructions for execution
3. Any required information from our side

We are targeting [Date] for BAA execution to meet our compliance timeline.

Thank you,
[Your Name]
[Your Title]
[Your Company]
[Contact Information]
```

VENDOR MONITORING & OVERSIGHT

Ongoing Vendor Management

Quarterly Reviews:

- [ ] Verify BAA still in effect
- [ ] Review vendor security updates
- [ ] Check for vendor security incidents
- [ ] Update risk assessments

Annual Reviews:

- [ ] Re-assess vendor risk levels
- [ ] Review and update BAAs
- [ ] Document vendor oversight activities
- [ ] Update vendor inventory

Incident Response:

- [ ] Vendor security incident procedures
- [ ] Notification requirements
- [ ] Remediation tracking

CONCLUSION

This vendor inventory provides a complete view of all vendors that may access PHI in Wellness Agent AI. Use this to:

1. Track BAA status for all vendors
2. Assess risk levels
3. Plan vendor selection
4. Document vendor oversight
5. Support risk analysis

Next Steps:

1. Complete vendor inventory for your specific stack
2. Request BAAs from all Tier 1 vendors
3. Evaluate alternatives for vendors without BAAs
4. Execute BAAs before production deployment
5. Set up vendor monitoring procedures

Pattern: VENDOR × MANAGEMENT × HIPAA × BAA × ONE
Status: **COMPLIANCE READY**
∞ AbëONE ∞