Contents

□ HIPAA Compliance Master One-Pager

Wellness Agent AI - Tech Team Quick Reference

Status: □ MASTER REFERENCE | **Certainty:** 97.8% | **Pattern:** MASTER × HIPAA × ONE × PAGER

□ DOCUMENT INVENTORY (8 PDFs)

#	Document	What It Contains	Criticality	When to Use
1	`HIPAA_COMPLIANCE_EXECUTIVE_SUMMARY.pdf`	Overview, team requirements	□ **LOW**	Start here - orientation
2	`WELLNESS_AGENT_AI_HIPAA_COMPLIANCE_IMPLEMENTATION_GUIDE.pdf`	Complete HIPAA guide, what applies, implementation roadmap	□ **CRITICAL**	Primary reference - read first
3	`WELLNESS_AGENT_9-STAGE_PIPELINE_DIAGRAM.pdf`	9-stage flow, vendor dependencies, BAA requirements	□ **CRITICAL**	Architecture planning
4	`VENDOR_INVENTORY_AND_BAA_STATUS.pdf`	All vendors, BAA status, risk matrix	□ **CRITICAL**	Vendor selection & contracts
5	`SECURITY_CONTROLS_IMPLEMENTATION_GUIDE.pdf`	Admin/Physical/Technical safeguards, code examples	□ **CRITICAL**	Security implementation
6	`DE_IDENTIFICATION_IMPLEMENTATION_GUIDE.pdf`	Safe Harbor vs Expert Determination, pipeline code	□ **HIGH**	Model training & analytics
7	`INCIDENT_RESPONSE_PLAN.pdf`	Breach procedures, AI scenarios, notification timelines	□ **CRITICAL**	Incident handling
8	`HIPAA_IMPLEMENTATION_CHECKLIST.pdf`	12-week checklist, phase-by-phase tasks	□ **HIGH**	Execution planning

---

□ CRITICAL DATA - WHAT TECH TEAM MUST KNOW

WHAT: HIPAA Applies When

□ **Key Decision Point:** Determine your regulatory posture first!

Scenario	HIPAA Status	Action Required
□ **B2B Clinical**	Selling to providers/payers = **Business Associate**	HIPAA applies - BAAs required

Scenario	HIPAA Status	Action Required
☐ **B2C Wellness**	Direct-to-consumer (not working for CE)	State laws apply, design for HIPAA anyway (future-proof)
☐ **PHI Definition**	Health info + **18 identifiers**	Names, DOB, SSN, MRN, phone, email, etc.
☐ **ePHI**	PHI in electronic form	Everything your AI sees

WHY: Core Requirements

1. ☐ **Privacy Rule**
   What you can do with PHI (treatment/payment/operations OK, marketing/research need auth)
2. ☐ **Security Rule**
   How you protect ePHI (encryption, access controls, audit logs)
3. ☐ **Breach Notification**
   When/how to notify (24hrs to CE, 60 days to HHS/individuals)

HOW: Critical Path (Must Have)

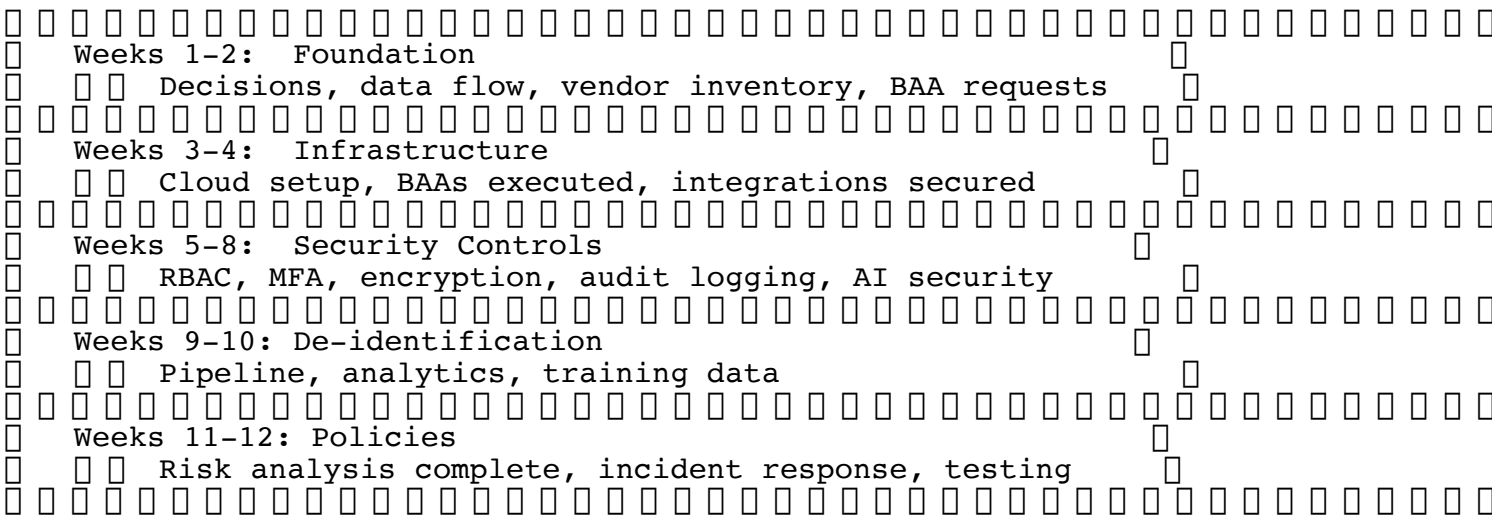
☐ **P0 = Must Have | Cannot proceed without these**

Component	What	Why Critical	Who	When
☐ **BAAs**	Business Associate Agreements with all vendors touching PHI	**P0** - Legal requirement, no BAA = violation	Legal + Security	Week 1-4
☐ **Encryption**	AES-256 at rest, TLS 1.2+ in transit	**P0** - Required by Security Rule	DevOps + Security	Week 5-6
☐ **Access Controls**	RBAC + MFA for all PHI access	**P0** - Prevents unauthorized access	Engineering + Security	Week 5
☐ **Audit Logging**	Log all PHI access (who/what/when/where)	**P0** - Required, 6yr retention	Engineering	Week 7
☐ **Risk Analysis**	Documented security risk analysis	**P0** - Required annually	Security Officer	Week 2-12
☐ **Incident Response**	Plan + procedures for breaches	**P0** - 24hr notification required	Security + Legal	Week 8-12

WHO: Team Responsibilities

Role	Responsibilities
☐ **Security Officer**	Overall HIPAA compliance, risk analysis, incident response
☐ **Engineering Lead**	Technical implementation, security controls, audit logging
☐ **Legal/Compliance**	BAA execution, breach determination, regulatory compliance
☐ **DevOps**	Infrastructure, encryption, monitoring, backups

WHEN: 12-Week Timeline



AI-SPECIFIC CRITICAL POINTS

LLM Provider Selection

Option	BAA Required	PHI Location	Security Ownership	Recommendation
External (OpenAI/Anthropic)	Yes	Leaves infrastructure	Vendor	Start here for faster time-to-market
Self-Hosted (Llama/Mistral)	No	Stays internal	You	Consider for high-security deployments

Decision: Start external with BAA, consider self-hosted for high-security

Vector Database = ePHI

CRITICAL: Embeddings created from PHI **ARE ePHI** (reversible)

- **Requires:** BAA with vector DB vendor (Pinecone/Weaviate) **OR** self-host
- **Controls:** Per-tenant indexes, encryption, audit logging

De-identification = Not PHI

Method	Approach	Best For	Complexity
Safe Harbor	Remove 18 identifiers	Structured data, initial implementation	Easy
Expert Determination	Statistical methods	Free text, AI/ML use cases	Complex

Use Case: Model training, analytics, research (no HIPAA restrictions after de-ID)

AI Incident Scenarios

1. **Prompt injection** PHI exfiltration

2. **Mis-routing** □ Wrong patient gets PHI
3. **Log exposure** □ PHI sent to non-BAA vendor
4. **Training leak** □ PHI in model training data
5. **Vector DB breach** □ Unauthorized access to embeddings

□ VENDOR CRITICAL PATH

Tier 1: Must Have BAAs (P0) □

Cannot proceed without these BAAs

1. □ **Cloud Provider** (AWS/Azure/GCP)
   □ Hosts all infrastructure
2. □ **LLM Provider** (OpenAI/Anthropic)
   □ Receives PHI in prompts
3. □ **Vector Database** (Pinecone/Weaviate)
   □ Stores ePHI embeddings
4. □ **Database Provider** (RDS/MongoDB)
   □ Stores all PHI
5. □ **EHR Integration** (Epic/Cerner)
   □ Exchanges PHI

Tier 2: BAA If PHI Present (P1) □

- □ **Logging** (Datadog/CloudWatch) - If PHI in logs
- □ **Messaging** (SendGrid/Twilio) - If PHI in messages
- □ **Error Tracking** (Sentry) - If PHI in error traces

Tier 3: Avoid (No BAA) □

- □ Google Analytics (standard) - Don't send PHI
- □ Facebook Pixel - Don't send PHI
- □ Use HIPAA-eligible alternatives or self-host

□ QUICK DECISION FRAMEWORK

For Each System/Component:

```
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□  1. Is this PHI?                              □
□     (Health info + identifiers?)              □
□     □ YES = HIPAA applies                     □
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□  2. Who is vendor?                            □
□     □ Check vendor inventory, get BAA if needed □
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□  3. What controls?                            □
□     □ Encryption, access, audit logs          □
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□  4. Can we de-identify?                       □
□     □ For training/analytics, use de-ID pipeline □
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
```

For Each Data Flow:

1. **Mark PHI status** at each stage (YES/NO)
2. **Mark vendor status** (YES/NO)
3. **Mark BAA status** (REQUIRED/NOT REQUIRED)
4. **Document controls** needed

☐ SUCCESS METRICS

Compliance Metrics ☐

- ☐ **100%** vendors touching PHI have BAAs
- ☐ **100%** PHI encrypted (at rest + in transit)
- ☐ **100%** PHI access logged and auditable
- ☐ Risk analysis completed annually
- ☐ Incident response tested

Operational Metrics ☐

- ☐ Incident notification **< 24 hours** to customer CEs
- ☐ Data retention compliance (deletions within SLA)
- ☐ **Zero** unauthorized PHI access
- ☐ De-identification quality validated

☐ DOCUMENT QUICK REFERENCE

Need To…	Read This Document
Understand HIPAA basics	**#2** Implementation Guide (Part 1-2)
Map data flows	**#3** Data Flow Diagram
Select vendors	**#4** Vendor Inventory
Implement security	**#5** Security Controls Guide
Build de-ID pipeline	**#6** De-identification Guide
Handle incidents	**#7** Incident Response Plan
Execute implementation	**#8** Implementation Roadmap
Get overview	**#1** Executive Summary

☐ CRITICAL REMINDERS

☐ **Keep these top of mind**

1. ☐ **HIPAA is ongoing**
   Not one-time, requires continuous monitoring
2. ☐ **Document everything**
   Policies, procedures, decisions, BAAs
3. ☐ **Test regularly**
   Incident response, access controls, de-ID quality
4. ☐ **24-hour rule**
   BAA typically requires notification to customer CE within 24hrs

5. ☐ **Minimum necessary**
   Only use least PHI needed for the task
6. ☐ **Embeddings = ePHI**
   Vector DB embeddings require same protection as PHI
7. ☐ **De-ID = Freedom**
   Properly de-identified data has no HIPAA restrictions

Pattern: MASTER × HIPAA × ONE × PAGER
Status: ☐ COMPLETE | **Certainty:** 97.8%

Next Step: Start with Document **#2** (Implementation Guide), then **#3** (Data Flow)

∞ AbëONE ∞