answara.ai

HEALTHCARE-READY COMPLIANCE

HIPAA Compliance Checklist

For Medical Practices, Dental Offices, Med Spas & Healthcare Organizations

This comprehensive checklist helps healthcare organizations implement HIPAA-compliant AI voice solutions. Use it to evaluate your readiness, track implementation progress, and ensure ongoing compliance with Protected Health Information (PHI) requirements.

500+	0	24 hr	SOC 2
HEALTHCARE CLIENTS	HIPAA VIOLATIONS	BAA TURNAROUND	TYPE II CERTIFIED

answara.ai
hipaa@answara.ai | answara.ai/hipaa

PRE-IMPLEMENTATION

Section 1 · Pre-Implementation Assessment

Complete these items before deploying any AI voice solution that will handle Protected Health Information.

1.1 Organizational Readiness

- [ ] Designated HIPAA Security Officer identified and documented
- [ ] Privacy Officer role assigned (may be same as Security Officer for small practices)
- [ ] Current HIPAA policies and procedures reviewed and up-to-date
- [ ] Staff HIPAA training completed within the last 12 months
- [ ] Risk assessment conducted within the last year
- [ ] Incident response plan documented and tested

1.2 Vendor Evaluation Criteria

- [ ] Vendor provides Business Associate Agreement (BAA)
- [ ] Vendor has SOC 2 Type II certification (or equivalent)
- [ ] Data encryption standards verified (AES-256 at rest, TLS 1.3 in transit)
- [ ] Vendor breach notification procedures reviewed (must be within 24 hours)
- [ ] Data retention and deletion policies documented
- [ ] Vendor security whitepaper or documentation obtained

> **PRO TIP**
>
> Request a copy of the vendor's SOC 2 report and have your IT team or consultant review it. Pay special attention to any exceptions or qualifications noted in the audit findings.

LEGAL & CONTRACTUAL

Section 2 · Business Associate Agreement

A BAA is legally required before any vendor can access, create, receive, or transmit PHI on your behalf.

2.1 Required BAA Elements

- [ ] Permitted uses and disclosures of PHI clearly defined
- [ ] Prohibition on unauthorized use or disclosure of PHI
- [ ] Requirement for appropriate safeguards to prevent unauthorized access
- [ ] Breach notification requirements and timelines specified
- [ ] Subcontractor requirements (vendor must ensure their subcontractors also comply)
- [ ] Requirement to make PHI available for patient access requests
- [ ] Amendment provisions for PHI corrections
- [ ] Accounting of disclosures requirement
- [ ] Right to terminate agreement for material breach
- [ ] Data return or destruction upon termination

2.2 BAA Execution Checklist

- [ ] BAA reviewed by legal counsel or compliance officer
- [ ] All services involving PHI are covered by the agreement
- [ ] Effective date established before any PHI access begins
- [ ] Signed copy retained in compliance documentation
- [ ] Annual review date scheduled for BAA renewal

TECHNICAL CONTROLS

Section 3 · Technical Safeguards

Verify these technical controls are in place to protect ePHI integrity and confidentiality.

3.1 Access Controls

- [ ] Unique user identification for all staff accessing the system
- [ ] Multi-factor authentication (MFA) enabled for all users
- [ ] Role-based access controls configured (minimum necessary access)
- [ ] Automatic session timeout configured (recommended: 15 minutes or less)
- [ ] Emergency access procedures documented
- [ ] SSO integration configured (if applicable)

3.2 Encryption Requirements

- [ ] AES-256 encryption at rest for all stored PHI
- [ ] TLS 1.3 encryption for all data in transit
- [ ] End-to-end call encryption for voice communications
- [ ] Hardware Security Module (HSM) for key management verified

3.3 Audit Controls

- [ ] Immutable audit logs enabled for all PHI access
- [ ] User access tracking configured and tested
- [ ] Data modification history retained
- [ ] Audit log export capability verified for compliance reporting
- [ ] Regular audit log review schedule established

POLICY & PEOPLE

Section 4 · Administrative Safeguards

Establish policies, procedures, and workforce management to ensure ongoing compliance.

4.1 Policies & Procedures

- [ ] AI voice system usage policy created and distributed to staff
- [ ] Patient communication protocols documented (what AI can/cannot discuss)
- [ ] Escalation procedures for sensitive inquiries established
- [ ] Data retention policy aligned with state and federal requirements
- [ ] Right to erasure procedures documented

4.2 Workforce Training

- [ ] Staff trained on HIPAA-compliant use of AI voice platform
- [ ] Training documentation and attendance records maintained
- [ ] New hire training process established
- [ ] Annual refresher training scheduled

4.3 Contingency Planning

- [ ] Backup communication procedures documented (if AI system is unavailable)
- [ ] Data backup verification completed
- [ ] Disaster recovery plan includes AI voice system

INFRASTRUCTURE

Section 5 · Physical Safeguards

Ensure the physical infrastructure protecting PHI meets HIPAA requirements.

- [ ] Vendor data centers are SOC 2 Type II certified
- [ ] 24/7 physical security monitoring at data centers
- [ ] Biometric or multi-factor access controls at data centers
- [ ] Environmental hazard protection (fire, flood, power) verified
- [ ] Secure equipment disposal procedures documented
- [ ] Isolated healthcare environment (data not commingled with non-healthcare)

INCIDENT PREPAREDNESS

Section 6 · Incident Response

Prepare for potential security incidents with documented response procedures.

6.1 Response Procedures

- [ ] Internal incident response team identified
- [ ] Vendor incident response contact information documented
- [ ] Breach notification timeline understood (60 days to HHS, 24 hours from vendor)
- [ ] State breach notification requirements documented
- [ ] Media notification procedures established (if breach affects 500+ individuals)

6.2 Documentation Requirements

- [ ] Incident documentation template created
- [ ] Root cause analysis procedures documented
- [ ] Corrective action tracking system established
- [ ] Post-incident reporting template available

> **IMPORTANT · BREACH NOTIFICATION TIMELINE**
>
> Under HIPAA, covered entities must notify affected individuals within 60 days of discovering a breach. Breaches affecting 500+ individuals must also be reported to local media. Ensure your vendor commits to notifying you within 24 hours of any suspected breach.

ROLLOUT PLAN

Section 7 · Implementation Timeline

Follow this recommended timeline for a compliant AI voice implementation.

Timeline	Phase	Key Activities
Day 1	**Initial Consultation**	Discuss healthcare needs and compliance requirements
Day 1–3	**BAA Execution**	Review, negotiate (if needed), and sign BAA
Day 3–5	**Secure Setup**	Configure HIPAA-compliant environment, encryption, access controls
Day 5–7	**Staff Training**	Train team on HIPAA-compliant platform usage
Day 7+	**Go Live**	Launch compliant AI receptionist with full audit logging

MAINTAIN COMPLIANCE

Section 8 · Ongoing Compliance

Maintain compliance with regular reviews and updates.

8.1 Regular Reviews

- [ ] **Monthly:** Review audit logs for unauthorized access attempts
- [ ] **Quarterly:** Test incident response procedures
- [ ] **Annually:** Conduct comprehensive risk assessment
- [ ] **Annually:** Review and update BAA if needed
- [ ] **Annually:** Complete staff HIPAA refresher training
- [ ] **As needed:** Update policies when regulations change

8.2 Documentation Retention

- [ ] BAA copies retained for 6 years from termination date
- [ ] Training records retained for 6 years
- [ ] Risk assessments retained for 6 years
- [ ] Incident documentation retained for 6 years
- [ ] Policy versions and change history maintained

BY PRACTICE TYPE

Section 9 · Specialty Considerations

Additional considerations for specific healthcare practice types.

Dental Practices

- Verify AI can integrate with practice management software (Dentrix, Eaglesoft, Open Dental)
- Configure appointment type recognition for hygiene vs. treatment visits
- Ensure insurance verification inquiries are handled compliantly

Medical Practices

- Configure triage protocols for urgent vs. routine calls
- Ensure prescription refill requests are handled appropriately
- Verify integration with EHR systems (Epic, Cerner, athenahealth)

Med Spas & Aesthetics

- Configure consultation vs. treatment appointment types
- Ensure pricing inquiries are handled per your policies
- Verify medical director oversight protocols are followed

Mental Health Practices

- Implement enhanced privacy protocols for sensitive communications
- Configure crisis intervention escalation procedures
- Ensure 42 CFR Part 2 compliance for substance abuse treatment

Physical Therapy

- Configure authorization tracking for visit limits
- Ensure patient portal integration for exercise programs
- Verify insurance pre-authorization inquiry handling

Specialty Clinics

- Configure specialty-specific appointment types
- Ensure referral coordination is handled compliantly
- Verify procedure-specific intake requirements

Ready for HIPAA-Compliant AI?

Join hundreds of healthcare organizations using answara.ai to automate patient communications while maintaining the highest standards of compliance.

Request BAA: hipaa@answara.ai

Live Demo: answara.ai/demo

YOUR ORGANIZATION

Notes & Action Items

Use this space to document specific action items, responsible parties, and deadlines for your organization.