https://www.cybersecurityservices.com
1-800-390-1053

Client HIPAA Policy Readiness Worksheet

Use the dropdowns to mark each policy area, then add evidence names, links, owners, or notes.

Client Information

Organization Name	Completed By	Date

Status Options

In Place	Current policy/procedure exists and supporting evidence is available.
Partially In Place	Some documentation exists, but it may be incomplete, outdated, or missing evidence.
Not in Place	No current policy/procedure or supporting evidence exists.
Not Applicable	The item does not apply; provide a brief explanation in the notes field.

Important Note on Addressable Items

Some HIPAA Security Rule implementation specifications are labeled addressable, but addressable does not mean optional. The organization must assess each addressable specification, implement it if reasonable and appropriate, or document why it is not reasonable and appropriate and implement an equivalent alternative measure if reasonable and appropriate.

Reference: 45 CFR § 164.306

Instructions

1. Select a status for every policy row using the dropdown field.
2. Use Evidence / Notes to identify file names, document owners, repository links, dates, or gap explanations.
3. If a policy is partially in place or not applicable, explain what is missing or why the item does not apply.
4. Save a completed copy and return it with the supporting documents requested in the evidence summary.

#	Policy / Procedure Area	What to Provide	Rule Reference	Status	Evidence / Notes
Core HIPAA Governance and Privacy Policies					
1	**HIPAA Privacy Policies and Procedures**	Written policies and procedures governing permitted uses, disclosures, safeguards, individual rights, complaints, workforce obligations, sanctions, mitigation, breach handling, and documentation.	45 CFR § 164.530	Select...	
2	**HIPAA Security Policies and Procedures**	Written policies and procedures implementing administrative, physical, and technical safeguards for electronic protected health information, or ePHI.	45 CFR § 164.316	Select...	
3	**Notice of Privacy Practices**	Current Notice of Privacy Practices, distribution process, website posting if applicable, and acknowledgment records where required.	45 CFR § 164.520	Select...	
4	**Privacy Officer Designation**	Documentation naming the privacy official responsible for developing and implementing privacy policies and procedures.	45 CFR § 164.530(a)	Select...	
5	**Security Officer Designation**	Documentation naming the security official responsible for Security Rule policies and procedures.	45 CFR § 164.308(a)(2)	Select...	
6	**HIPAA Training**	Training policy, training materials, new-hire training records, refresher training records, and training after material policy changes.	45 CFR § 164.530(b)	Select...	
7	**Security Awareness and Training**	Security awareness program covering periodic reminders, malware protection, login monitoring, and password management as applicable.	45 CFR § 164.308(a)(5)	Select...	
8	**Complaint Process**	Procedure for individuals to submit privacy complaints and evidence showing complaints and their disposition are documented.	45 CFR § 164.530(d)	Select...	
9	**Sanctions and Discipline**	Policy for applying sanctions to workforce members who violate HIPAA policies or HIPAA requirements, plus records of sanctions if any.	45 CFR § 164.530(e), 45 CF…	Select...	
10	**Mitigation**	Procedure for mitigating harmful effects of improper uses or disclosures of PHI or violations by the organization or a business associate.	45 CFR § 164.530(f)	Select...	
11	**Non-Retaliation**	Policy prohibiting intimidation, threats, coercion, discrimination, or retaliation against individuals exercising HIPAA rights or filing complaints.	45 CFR § 164.530(g)	Select...	
12	**No Waiver of Rights**	Policy confirming individuals are not required to waive HIPAA rights as a condition of treatment, payment, enrollment, or eligibility for benefits.	45 CFR § 164.530(h)	Select...	
13	**Policy Review, Updates, and Retention**	Document control process for reviewing, updating, approving, retaining, and making HIPAA policies available to responsible personnel.	45 CFR § 164.530(i)-(j), 45 …	Select...	
PHI Use, Disclosure, and Individual Rights Policies					
14	**Permitted Uses and Disclosures of PHI**	Policy explaining when PHI may be used or disclosed, including treatment, payment, health care operations, required disclosures, and other permitted disclosures.	HHS Privacy Rule Summary	Select...	
15	**Minimum Necessary**	Policy limiting uses, disclosures, and requests for PHI to the minimum necessary amount when the minimum necessary standard applies.	HHS Privacy Rule Summary	Select...	

#	Policy / Procedure Area	What to Provide	Rule Reference	Status	Evidence / Notes
PHI Use, Disclosure, and Individual Rights Policies					
16	**Role-Based Access to PHI**	Role-based access matrix or policy identifying which workforce roles need access to PHI, what PHI they need, and under what conditions.	HHS Privacy Rule Summary	Select...	
17	**Authorizations**	Authorization forms and procedures for uses and disclosures requiring written authorization, including revocation handling.	45 CFR § 164.520	Select...	
18	**Right of Access**	Procedure for individuals to inspect, obtain copies of, or request transmission of PHI where applicable.	45 CFR § 164.520	Select...	
19	**Amendment of PHI**	Procedure for individuals to request amendment of PHI.	45 CFR § 164.520	Select...	
20	**Accounting of Disclosures**	Procedure for individuals to request an accounting of disclosures.	45 CFR § 164.520	Select...	
21	**Request for Restrictions**	Procedure for individuals to request restrictions on certain uses and disclosures.	45 CFR § 164.520	Select...	
22	**Confidential Communications**	Procedure for individuals to request confidential communications by alternative means or at alternative locations.	45 CFR § 164.520	Select...	
23	**Privacy Safeguards for PHI in All Formats**	Administrative, physical, and technical privacy safeguards to protect PHI from intentional or unintentional improper use or disclosure and to limit incidental disclosures.	45 CFR § 164.530(c)	Select...	
Security Rule Administrative Safeguard Policies					
24	**Security Management Process**	Policies and procedures to prevent, detect, contain, and correct security violations.	45 CFR § 164.308(a)(1)	Select...	
25	**Risk Analysis**	Most recent HIPAA security risk analysis identifying risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	45 CFR § 164.308(a)(1)	Select...	
26	**Risk Management**	Risk treatment plan or policy showing how identified risks are reduced to a reasonable and appropriate level.	45 CFR § 164.308(a)(1)	Select...	
27	**Information System Activity Review**	Procedures and evidence for regular review of audit logs, access reports, and security incident tracking reports.	45 CFR § 164.308(a)(1)	Select...	
28	**Workforce Security**	Policies ensuring workforce members have appropriate access to ePHI and preventing access by workforce members who should not have it.	45 CFR § 164.308(a)(3)	Select...	
29	**Authorization and Supervision**	Procedures for authorizing and supervising workforce members who work with ePHI or in locations where ePHI may be accessed.	45 CFR § 164.308(a)(3)	Select...	
30	**Workforce Clearance**	Procedure for determining that workforce access to ePHI is appropriate.	45 CFR § 164.308(a)(3)	Select...	

#	Policy / Procedure Area	What to Provide	Rule Reference	Status	Evidence / Notes
Security Rule Administrative Safeguard Policies					
31	**Termination and Offboarding**	Procedure for removing ePHI access when employment or another workforce arrangement ends.	45 CFR § 164.308(a)(3)	Select...	
32	**Information Access Management**	Policies and procedures for authorizing access to ePHI consistent with Privacy Rule access requirements.	45 CFR § 164.308(a)(4)	Select...	
33	**Access Authorization**	Procedure for granting access to ePHI through workstations, systems, programs, transactions, or other mechanisms.	45 CFR § 164.308(a)(4)	Select...	
34	**Access Establishment and Modification**	Procedure to establish, document, review, and modify user access rights.	45 CFR § 164.308(a)(4)	Select...	
35	**Security Incident Response**	Procedure to identify, respond to, mitigate, and document suspected or known security incidents and outcomes.	45 CFR § 164.308(a)(6)	Select...	
36	**Contingency Plan**	Policies and procedures for responding to emergencies or other events that damage systems containing ePHI.	45 CFR § 164.308(a)(7)	Select...	
37	**Data Backup Plan**	Procedure to create and maintain retrievable exact copies of ePHI.	45 CFR § 164.308(a)(7)	Select...	
38	**Disaster Recovery Plan**	Procedure to restore lost data after a disruptive event.	45 CFR § 164.308(a)(7)	Select...	
39	**Emergency Mode Operation Plan**	Procedure to continue critical business processes while protecting ePHI during emergency operations.	45 CFR § 164.308(a)(7)	Select...	
40	**Contingency Plan Testing and Revision**	Procedure and records for periodic testing and revision of contingency plans when reasonable and appropriate.	45 CFR § 164.308(a)(7), 45 …	Select...	
41	**Application and Data Criticality Analysis**	Assessment of the relative criticality of applications and data supporting contingency planning when reasonable and appropriate.	45 CFR § 164.308(a)(7), 45 …	Select...	
42	**Security Evaluation**	Periodic technical and nontechnical evaluations of Security Rule compliance, including evaluations after environmental or operational changes affecting ePHI.	45 CFR § 164.308(a)(8)	Select...	
43	**Business Associate Management**	Policy requiring satisfactory assurances through written business associate contracts or other arrangements before a vendor creates, receives, maintains, or transmits ePHI on behalf of the organization.	45 CFR § 164.308(b)	Select...	
44	**Subcontractor / Downstream Business Associate Management**	For business associates, procedure requiring satisfactory assurances from subcontractors that create, receive, maintain, or transmit ePHI on their behalf.	45 CFR § 164.308(b)	Select...	
Security Rule Physical Safeguard Policies					
45	**Facility Access Controls**	Policies and procedures limiting physical access to electronic information systems and facilities while allowing authorized access.	45 CFR § 164.310(a)	Select...	

#	Policy / Procedure Area	What to Provide	Rule Reference	Status	Evidence / Notes
Security Rule Physical Safeguard Policies					
46	**Contingency Operations Facility Access**	Procedure allowing facility access in support of disaster recovery and emergency mode operations when reasonable and appropriate.	45 CFR § 164.310(a), 45 CF…	Select...	
47	**Facility Security Plan**	Policies and procedures to safeguard facilities and equipment from unauthorized physical access, tampering, and theft when reasonable and appropriate.	45 CFR § 164.310(a), 45 CF…	Select...	
48	**Access Control and Validation / Visitor Control**	Procedure to control and validate facility access based on role or function, including visitor control where applicable.	45 CFR § 164.310(a)	Select...	
49	**Facility Maintenance Records**	Procedure to document facility repairs and security-related modifications such as hardware, walls, doors, and locks where reasonable and appropriate.	45 CFR § 164.310(a), 45 CF…	Select...	
50	**Workstation Use**	Policy specifying proper workstation functions, how those functions are performed, and physical surroundings for workstations that access ePHI.	45 CFR § 164.310(b)	Select...	
51	**Workstation Security**	Physical safeguards restricting workstation access to authorized users.	45 CFR § 164.310(c)	Select...	
52	**Device and Media Controls**	Policies governing receipt, removal, and movement of hardware and electronic media containing ePHI into, out of, and within facilities.	45 CFR § 164.310(d)	Select...	
53	**Media Disposal**	Procedure for final disposition of ePHI and hardware or electronic media on which ePHI is stored.	45 CFR § 164.310(d)	Select...	
54	**Media Re-Use**	Procedure for removing ePHI from electronic media before media are made available for re-use.	45 CFR § 164.310(d)	Select...	
55	**Hardware and Media Accountability**	Records of hardware and electronic media movement and the responsible person when reasonable and appropriate.	45 CFR § 164.310(d), 45 CF…	Select...	
56	**Device and Media Backup Before Movement**	Procedure to create retrievable exact copies of ePHI before equipment movement when needed and reasonable.	45 CFR § 164.310(d), 45 CF…	Select...	
Security Rule Technical Safeguard Policies					
57	**Technical Access Controls**	Technical policies and procedures allowing ePHI system access only to authorized persons or software programs.	45 CFR § 164.312(a)	Select...	
58	**Unique User Identification**	Procedure assigning a unique name or number for identifying and tracking user identity.	45 CFR § 164.312(a)	Select...	
59	**Emergency Access**	Procedure for obtaining necessary ePHI during an emergency.	45 CFR § 164.312(a)	Select...	
60	**Automatic Logoff**	Electronic procedure terminating sessions after inactivity when reasonable and appropriate.	45 CFR § 164.312(a), 45 CF…	Select...	

#	Policy / Procedure Area	What to Provide	Rule Reference	Status	Evidence / Notes
Security Rule Technical Safeguard Policies					
61	**Encryption and Decryption**	Policy and documented decision process for encrypting and decrypting ePHI where reasonable and appropriate.	45 CFR § 164.312(a), 45 CF…	Select...	
62	**Audit Controls**	Hardware, software, or procedural mechanisms that record and examine activity in systems containing or using ePHI.	45 CFR § 164.312(b)	Select...	
63	**Integrity Controls**	Policies and procedures protecting ePHI from improper alteration or destruction.	45 CFR § 164.312(c)	Select...	
64	**ePHI Authentication / Integrity Verification**	Mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner when reasonable and appropriate.	45 CFR § 164.312(c), 45 CF…	Select...	
65	**Person or Entity Authentication**	Procedure to verify that a person or entity seeking access to ePHI is the one claimed.	45 CFR § 164.312(d)	Select...	
66	**Transmission Security**	Technical security measures guarding against unauthorized access to ePHI transmitted over electronic communications networks.	45 CFR § 164.312(e)	Select...	
67	**Transmission Integrity Controls**	Security measures to ensure electronically transmitted ePHI is not improperly modified without detection until disposed of when reasonable and appropriate.	45 CFR § 164.312(e), 45 CF…	Select...	
68	**Transmission Encryption**	Mechanism to encrypt transmitted ePHI whenever deemed appropriate.	45 CFR § 164.312(e)	Select...	
Breach Notification Policies					
69	**Breach Identification and Risk Assessment**	Procedure for evaluating impermissible PHI uses or disclosures, including the four-factor breach risk assessment and documentation of conclusions.	45 CFR § 164.402	Select...	
70	**Individual Breach Notification**	Procedure and templates for notifying affected individuals without unreasonable delay and no later than 60 calendar days after breach discovery.	45 CFR § 164.404	Select...	
71	**Media Breach Notification**	Procedure for notifying prominent media outlets when a breach involves more than 500 residents of a state or jurisdiction.	45 CFR § 164.406	Select...	
72	**HHS Breach Notification**	Procedure for notifying HHS for breaches involving 500 or more individuals and maintaining/logging/reporting breaches involving fewer than 500 individuals.	45 CFR § 164.408	Select...	
73	**Business Associate Breach Notification**	For business associates, procedure to notify the covered entity of a breach without unreasonable delay and no later than 60 calendar days after discovery.	45 CFR § 164.410	Select...	
74	**Breach Documentation and Burden of Proof**	Documentation showing required notifications were made or why an incident did not constitute a reportable breach.	45 CFR § 164.414	Select...	

Evidence Request Summary

Governance	Privacy Officer designation, Security Officer designation, policy approvals, review dates, policy version history.
Risk Management	HIPAA security risk analysis, risk register, remediation plan, accepted risk records, security evaluation results.
Training	HIPAA privacy training records, security awareness records, new-hire training, retraining after material policy changes.
Access Management	Role-based access matrix, provisioning records, access reviews, termination checklists, privileged access records.
Incident and Breach	Incident response plan, incident logs, breach risk assessments, breach notification templates, HHS reporting logs.
Vendor Management	Business Associate Agreements, vendor inventory, subcontractor list, vendor risk reviews, vendor termination process.
Technical Safeguards	Audit log reviews, encryption settings, authentication configuration, backup records, disaster recovery test results.
Physical Safeguards	Facility access procedures, visitor logs, workstation security rules, media disposal records, device inventory.
Documentation	Current policy manual, procedures, templates, records, retention schedule, signed workforce acknowledgments.