HIPAA

Compliance Assessment Questionnaire

57 Assessment Questions • 14 Control Domains

ORGANIZATION INFORMATION

Organization Name: _____

Assessment Date: _____

Assessor Name / Title: _____

System / Scope: _____

SCORING METHOD

- ☐ **YES** (2 points) — Fully implemented — control is in place, documented, and operating effectively.
- ☐ **PARTIAL** (1 point) — Partially implemented — some elements are in place but gaps remain.
- ☐ **NO** (0 points) — Not implemented — control is missing or not operating.

Compliance Score = (Total Points ÷ Maximum Points) × 100%

Maximum possible points: 114 (57 questions × 2 points each)

SECURITY MANAGEMENT PROCESS

Reference: 45 CFR § 164.308(a)(1)

Q1 [45 CFR § 164.308(a)(1)(ii)(A)]

Have you conducted a risk analysis to identify potential risks to electronic protected health information (ePHI)?

OCR auditors will look for documentation of the risk analysis, including identified threats and vulnerabilities.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q2 [45 CFR § 164.308(a)(1)(ii)(B)]

Is there a risk management plan in place to address identified vulnerabilities?

OCR auditors will verify if a plan exists and is implemented to reduce risks to an acceptable level.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q3 [45 CFR § 164.308(a)(1)(ii)(C)]

Are sanctions in place for workforce members who fail to comply with security policies?

OCR auditors will examine if there are clear sanctions policies and if they are enforced.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q4 [45 CFR § 164.308(a)(8)]

Is there a process for periodic review and updates of security measures?

OCR will look at documentation of periodic review processes and updates.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q5 [45 CFR § 164.308(a)(1)]

Has the organization assigned responsibility for risk analysis and management to specific personnel?

OCR auditors will confirm that risk management responsibilities are clearly assigned.

☐ YES ☐ PARTIAL ☐ NO Explanation:

ASSIGNED SECURITY RESPONSIBILITY

Reference: 45 CFR § 164.308(a)(2)

Q6 [45 CFR § 164.308(a)(2)]

Is there a designated security official responsible for overseeing HIPAA security policies?

OCR auditors expect a named individual with documented responsibilities.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q7 [45 CFR § 164.308(a)(2)]

Does the security official have adequate authority to implement and enforce security policies?

OCR will assess if the official has the organizational support and resources needed.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q8 [45 CFR § 164.308(a)(2)]

Is the security official's role clearly communicated to the workforce?

OCR auditors will look for evidence such as organizational charts or internal communications.

☐ YES ☐ PARTIAL ☐ NO Explanation:

WORKFORCE SECURITY

Reference: 45 CFR § 164.308(a)(3)

Q9 [45 CFR § 164.308(a)(3)(ii)(A)]

Are there authorization and supervision measures for workforce members who access ePHI?

OCR auditors will verify the presence of documented access controls and supervisory responsibilities.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q10 [45 CFR § 164.308(a)(3)(ii)(B)]

Does the organization have procedures to determine workforce member access authorization based on their roles?

OCR expects role-based access controls with clear documentation.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q11 [45 CFR § 164.308(a)(3)(ii)(C)]

Are there protocols for terminating workforce member access to ePHI upon separation from the organization?

OCR will examine policies and records of deactivating access privileges upon termination.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q12 [45 CFR § 164.308(a)(3)(ii)]

Is there a regular review of workforce access to ensure compliance with policies?

OCR auditors will check for documentation and evidence of regular access audits.

☐ YES ☐ PARTIAL ☐ NO Explanation:

INFORMATION ACCESS MANAGEMENT

Reference: 45 CFR § 164.308(a)(4)

Q13 [45 CFR § 164.308(a)(4)(ii)(A)]

Does the organization have policies to authorize access to ePHI only to those with a need to know?

OCR expects documented access policies reflecting minimum necessary access principles.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q14 [45 CFR § 164.308(a)(4)(ii)(B)]

Is there a formal process to establish and modify user access based on changes in job roles?

OCR auditors will look for evidence of processes that review and adjust access permissions.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q15 [45 CFR § 164.308(a)(4)(ii)(C)]

Are emergency access procedures in place for ePHI?

OCR expects documented procedures for granting emergency access when necessary.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q16 [45 CFR § 164.308(a)(4)]

Is access to information systems with ePHI reviewed periodically?

OCR will review records of regular access reviews to confirm compliance.

☐ YES ☐ PARTIAL ☐ NO Explanation:

SECURITY AWARENESS AND TRAINING

Reference: 45 CFR § 164.308(a)(5)

Q17 [45 CFR § 164.308(a)(5)(i)]

Are periodic security reminders provided to the workforce?

OCR auditors will expect records of security reminders, such as emails or training sessions.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q18 [45 CFR § 164.308(a)(5)(ii)(B)]

Is malware protection included in the organization's security training?

OCR will check for training materials and courses that cover malware protection.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q19 [45 CFR § 164.308(a)(5)(ii)(C)]

Does the organization monitor user logins for suspicious activity?

OCR expects documentation of login monitoring procedures and any follow-up actions taken.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q20 [45 CFR § 164.308(a)(5)(ii)(D)]

Are password management measures included in security training?

OCR will verify training materials include password creation and management best practices.

☐ YES ☐ PARTIAL ☐ NO Explanation:

SECURITY INCIDENT PROCEDURES

Reference: 45 CFR § 164.308(a)(6)

Q21 [45 CFR § 164.308(a)(6)(ii)]

Does the organization have an incident response plan for security breaches?

OCR auditors will look for a formal, documented incident response plan.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q22 [45 CFR § 164.308(a)(6)(ii)(A)]

Are there procedures to identify and respond to suspected or known security incidents?

OCR expects clear procedures for identifying, reporting, and mitigating incidents.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q23 [45 CFR § 164.308(a)(6)(ii)(C)]

Is there a process for documenting and reporting incidents and their outcomes?

OCR will look for incident logs and reports including actions taken.

☐ YES ☐ PARTIAL ☐ NO Explanation:

CONTINGENCY PLANNING

Reference: 45 CFR § 164.308(a)(7)

Q24 [45 CFR § 164.308(a)(7)(ii)(A)]

Does the organization have a data backup plan for ePHI?

OCR expects to see documented and implemented data backup procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q25 [45 CFR § 164.308(a)(7)(ii)(B)]

Is there a disaster recovery plan to restore lost ePHI?

OCR will review formal recovery plans and evidence of their testing.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q26 [45 CFR § 164.308(a)(7)(ii)(C)]

Are emergency operation procedures in place to address interruptions to business operations?

OCR auditors will look for procedures that ensure continuity of operations.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q27 [45 CFR § 164.308(a)(7)(ii)(D)]

Is the contingency plan tested and revised as necessary?

OCR will verify evidence of regular testing and revisions based on test results.

☐ YES ☐ PARTIAL ☐ NO Explanation:

EVALUATION

Reference: 45 CFR § 164.308(a)(8)

Q28 [45 CFR § 164.308(a)(8)]

Is there a process for periodic evaluation of security policies and procedures?

OCR expects documentation of regular evaluations and updates based on findings.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q29 [45 CFR § 164.308(a)(8)]

Have evaluations been conducted following material changes to operations or security practices?

OCR will look for reports or records of evaluations conducted post-changes.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q30 [45 CFR § 164.308(a)(8)]

Are evaluation results documented and used to improve security measures?

OCR auditors will expect evidence of documented evaluations and subsequent improvements.

☐ YES ☐ PARTIAL ☐ NO Explanation:

BUSINESS ASSOCIATE AGREEMENTS

Reference: 45 CFR § 164.308(b)

Q31 [45 CFR § 164.308(b)(1)]

Are there documented Business Associate Agreements (BAAs) with all relevant third parties?

OCR will verify the presence of signed BAAs for all third-party service providers handling ePHI.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q32 [45 CFR § 164.308(b)(1)]

Do the BAAs specify the responsibilities of business associates regarding ePHI protection?

OCR auditors will look for language within BAAs outlining specific security responsibilities.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q33 [45 CFR § 164.308(b)(2)]

Are BAAs reviewed and updated as necessary to reflect changes in the relationships or regulations?

OCR will review evidence of periodic BAA reviews and updates.

☐ YES ☐ PARTIAL ☐ NO Explanation:

PHYSICAL SAFEGUARDS

Reference: 45 CFR § 164.310

Q34 [45 CFR § 164.310(a)(1)]

Are there policies governing facility access to protect locations housing ePHI?

OCR auditors expect documented and enforced facility access policies.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q35 [45 CFR § 164.310(b)]

Are workstation use guidelines established for protecting ePHI?

OCR will check for policies regarding secure workstation use in compliance with HIPAA.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q36 [45 CFR § 164.310(c)]

Do security measures exist to safeguard workstations where ePHI is accessed?

OCR expects physical and technical controls to limit workstation access.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q37 [45 CFR § 164.310(d)(1)]

Are there controls over the receipt and removal of hardware and electronic media containing ePHI?

OCR will verify documented media control policies and practices.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q38 [45 CFR § 164.310(d)(2)(i)]

Is there a process for data backup and storage of electronic media?

OCR auditors will look for backup procedures ensuring the security of ePHI during media movement.

☐ YES ☐ PARTIAL ☐ NO Explanation:

TECHNICAL SAFEGUARDS

Reference: 45 CFR § 164.312

Q39 [45 CFR § 164.312(a)(1)]

Are access controls in place to allow only authorized users to access ePHI?

OCR expects technical measures ensuring that only authorized users have ePHI access.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q40 [45 CFR § 164.312(b)]

Are audit controls implemented to record and examine activities in information systems containing ePHI?

OCR will look for logs and audit tracking measures capturing system activities.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q41 [45 CFR § 164.312(c)(1)]

Is there a mechanism to ensure the integrity of ePHI by protecting it from improper alteration or destruction?

OCR auditors will verify technical measures preserving ePHI integrity.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q42 [45 CFR § 164.312(d)]

Are authentication measures in place to verify the identity of users attempting to access ePHI?

OCR expects secure authentications, such as passwords or biometrics.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q43 [45 CFR § 164.312(e)(1)]

Is transmission security in place to protect ePHI being transmitted over electronic communications networks?

OCR will look for encryption and other secure methods for ePHI transmission.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q44 [45 CFR § 164.312(a)(2)(iii)]

Are automatic logoff mechanisms deployed to prevent unauthorized access to ePHI?

OCR expects automatic logoff features configurated on systems accessing ePHI.

☐ YES ☐ PARTIAL ☐ NO Explanation:

PRIVACY RULE

Reference: 45 CFR § 164.500

Q45 [45 CFR § 164.520]

Is there a Notice of Privacy Practices (NPP) provided to patients and publicly posted?

OCR expects an accurate and accessible NPP communicated to individuals.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q46 [45 CFR § 164.514(d)]

Does the organization apply the 'minimum necessary' standard to uses and disclosures of PHI?

OCR will examine policies ensuring minimal PHI required is accessed or disclosed.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q47 [45 CFR § 164.524]

Are there procedures for individuals to access their PHI upon request?

OCR auditors expect documented and implemented processes for patient access requests.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q48 [45 CFR § 164.522]

Do patients have the ability to request restrictions on how their PHI is used or disclosed?

OCR will look for processes allowing individuals to make privacy restriction requests.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q49 [45 CFR § 164.506]

Are there clear policies for the use and disclosure of PHI for treatment, payment, and health care operations?

OCR expects clear and compliant PHI use and disclosure policies according to regulations.

☐ YES ☐ PARTIAL ☐ NO Explanation:

BREACH NOTIFICATION

Reference: 45 CFR §§ 164.400-414

Q50 [45 CFR § 164.402]

Are there procedures to identify and evaluate potential breaches of unsecured PHI?

OCR auditors will look for processes and criteria used to assess potential PHI breaches.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q51 [45 CFR § 164.404]

Are breach notifications provided to affected individuals in a timely manner?

OCR will verify evidence of timely notifications consistent with breach requirements.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q52 [45 CFR § 164.408]

Are breach incidents assessed to determine the necessity of notification to HHS?

OCR expects documented assessments of breach size and type to determine HHS reporting.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q53 [45 CFR § 164.410]

Is there a timeline and process for notifying media when a breach affects over 500 residents?

OCR will confirm if appropriate media notice procedures are in place and followed.

☐ YES ☐ PARTIAL ☐ NO Explanation:

DOCUMENTATION AND POLICIES

Reference: 45 CFR § 164.316

Q54 [45 CFR § 164.316(b)(1)]

Are security policies and procedures documented in writing or electronically?

OCR expects comprehensive written or electronic documentation of security policies.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q55 [45 CFR § 164.316(b)(2)(i)]

Is there a process to regularly review and update policies as needed?

OCR auditors will look for scheduled review cycles and updates of documentation.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q56 [45 CFR § 164.316(b)(2)(ii)]

Are security measures and policies retained for at least six years?

OCR requires evidence of proper retention schedules and practices for documentation.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q57 [45 CFR § 164.316]

Are HIPAA training records for workforce members maintained and accessible?

OCR expects documented records of HIPAA training activities for each workforce member.

☐ YES ☐ PARTIAL ☐ NO Explanation:

COMPLIANCE SCORE SUMMARY

Control Domain	Questions	Points Earned	Max Points	Score %
Security Management Process	5	___	10	___ %
Assigned Security Responsibility	3	___	6	___ %
Workforce Security	4	___	8	___ %
Information Access Management	4	___	8	___ %
Security Awareness and Training	4	___	8	___ %
Security Incident Procedures	3	___	6	___ %
Contingency Planning	4	___	8	___ %
Evaluation	3	___	6	___ %
Business Associate Agreements	3	___	6	___ %
Physical Safeguards	5	___	10	___ %
Technical Safeguards	6	___	12	___ %
Privacy Rule	5	___	10	___ %
Breach Notification	4	___	8	___ %
Documentation and Policies	4	___	8	___ %
TOTAL	**57**	___	**114**	___ **%**

SCORE INTERPRETATION

- **90–100% — Strong Compliance**
  Organization demonstrates robust controls across all domains. Minor improvements may be needed.
- **70–89% — Moderate Compliance**
  Most controls are in place but notable gaps exist. Remediation plan recommended within 90 days.
- **50–69% — Partial Compliance**
  Significant gaps in compliance posture. Prioritized remediation required. Consider engaging a consultant.
- **Below 50% — Non-Compliant**
  Organization does not meet minimum compliance requirements. Immediate action required.

ATTESTATION

Assessed by: _____ Signature: _____

Title: _____ Date: _____

Reviewed by: _____ Signature: _____

Title: _____ Date: _____

authorized auditor) for official compliance validation.