
CYBER360 / SPECIALIST SERVICES

HIPAA Compliance

Practical safeguards. Patient trust.

Build a practical approach to protecting health information. Cyber360 helps covered entities and business associates assess HIPAA gaps, manage security risks and put privacy, security and breach-response procedures into everyday operation.

01 Clear scope

02 Practical evidence

03 Priorities for improvement

TRUSTED SECURITY ADVISORY

Advice that leads to action.

cyber360.co | info@cyber360.co | Healthcare privacy & security

01 / SCOPE & FOCUS

The right question. A useful assessment.

Build a practical approach to protecting health information. Cyber360 helps covered entities and business associates assess HIPAA gaps, manage security risks and put privacy, security and breach-response procedures into everyday operation.

Applicability, scope & gap assessment

Covered-entity and business-associate roles, PHI flows, systems, facilities and contractual relationships.

A scope statement, gap assessment and prioritised implementation roadmap.

Security risk analysis & management

Agreed ePHI repositories, systems, users, interfaces, threats, vulnerabilities and existing controls.

A documented risk analysis, risk register and treatment plan with owners and review dates.

Administrative, physical & technical safeguards

Access, authentication, audit logging, integrity, transmission protection, facilities, workstations and media.

Safeguard recommendations, implementation guidance and agreed validation activities.

Privacy practices & individual rights

Permitted uses and disclosures, applicable minimum-necessary practices, notices, authorisations and rights workflows.

A tailored privacy documentation library and practical request-handling procedures.

Business associates & workforce

Business associates, relevant subcontractors, agreements, supplier oversight and role-specific training.

A business-associate inventory, agreement review actions and workforce training materials.

Breach readiness & continuous review

Incident escalation, investigation, breach assessment, notification processes and evidence maintenance.

A breach-response protocol, decision templates and ongoing compliance review calendar.

02 / APPROACH & DELIVERABLES

From agreed scope to practical action.

Define the scope

Confirm your role, activities, PHI flows and the systems and relationships to review.

Assess the evidence

Review policies, safeguards, workforce practices and existing compliance documentation.

Analyse the risk

Identify ePHI threats and vulnerabilities and prioritise risks with accountable owners.

Build the programme

Develop agreed policies, risk treatments, safeguard guidance and operational workflows.

Prepare people & response

Deliver role-based awareness and walk through privacy and breach-response responsibilities.

Review & improve

Maintain evidence, track remediation and reassess following material operational or technology changes.

WHAT YOU RECEIVE

For leadership & compliance owners

- Applicability and scope statement with a HIPAA gap assessment.
- Documented security risk analysis and risk treatment roadmap.
- Privacy and security governance responsibilities and policy actions.
- Compliance review calendar and workforce training materials.

For operational & technical teams

- PHI/ePHI flow and asset documentation for the agreed environment.
- Safeguard implementation guidance and validation priorities.
- Privacy-rights procedures and business-associate review toolkit.
- Incident escalation, breach assessment and notification templates.

03 / PREPARATION & NEXT STEPS

Start with the right context.

Role & relationships

- Describe healthcare activities and covered-entity or business-associate relationships.
- Share existing agreements and partner assurance requirements.

Information & systems

- List PHI and ePHI repositories, clinical systems, suppliers and data flows.
- Provide relevant architecture, asset inventories and access information.

Policies & evidence

- Share risk analyses, policies, training records and prior findings.
- Identify privacy, security, clinical, IT and operational owners.

Delivery & approvals

- Agree review boundaries, implementation tasks and change windows.
- Confirm legal review, decision authority and acceptance criteria.

PRACTICAL QUESTIONS

Who must comply with HIPAA?

HIPAA applies to covered entities and business associates as defined by US law. We assess your activities and relationships to establish relevant obligations; handling health data alone does not automatically establish applicability.

HIPAA is a US framework. Consulting does not provide HHS approval, certification or a guarantee of compliance. Specialist legal advice is separately agreed.

Reference: HHS HIPAA guidance for professionals (October 2026).

What is the difference between PHI and ePHI?

Protected health information is individually identifiable health information within HIPAA scope. The Privacy Rule covers PHI in different forms; the Security Rule focuses on electronic PHI and its administrative, physical and technical safeguards.

LET'S DISCUSS YOUR PRIORITIES

info@cyber360.co | cyber360.co

Contact Cyber360 to discuss your requirements.