The IBM Internet Security Systems approach for Health Insurance Portability and Accountability Act compliance overview
Health Insurance Portability and Accountability Act security requirements made simple

Protecting the confidentiality, integrity and availability of patient information is not just a best practice for healthcare organizations, but also a legal requirement. The Health Insurance Portability and Accountability Act (HIPAA) mandates all healthcare organizations effectively meet administrative, technical and physical safeguards to protect the privacy of patient information, and to maintain data integrity for employees, customers and shareholders.

The business challenges associated with achieving this level of security and HIPAA compliance, are abundant, include:

- Lack of dedicated security budget.
- Absence of necessary security expertise.
- Inability to easily deploy and manage required technology.
- Tight deadline in which to achieve compliance.
- Lack of employee education on security Best practices.

IBM Internet Security Systems™ (ISS) has demonstrated proven success helping organizations quickly and simply achieve HIPAA security mandates with:

- IBM Internet Security Systems Professional Security Services to help plan and implement security solutions.
- World-class protection technology from IBM Internet Security Systems protection platform to protect critical information assets from an ever-changing spectrum of threats and misuse.
- Comprehensive IBM Managed Protection Services (MPS) that adapt to a company’s varying budget and security issues.

- Up-to-the-minute security intelligence on the latest threats – collected by the IBM (ISS) team of security researchers. As part of the five-step process defined below, IBM ISS offers healthcare organizations the following to help meet the administrative, technical and physical safeguards of HIPAA security requirements:
- Professional Security Services – An elite team of security professionals that partner with organizations to assess current security posture and help develop a roadmap for meeting HIPAA security requirements.
- IBM protection platform – Comprises IBM ISS award winning solutions, which span the network, server and desktop environments as well as vulnerability detection applications. The IBM SiteProtector™ system central management application unifies configuration, deployment and data correlation for all of these agents.
- Managed Protection Services (MPS) – Provides around-the-clock protection for healthcare organizations lacking the time, expertise or appropriate internal resources to secure critical information. This comprehensive suite of services provides cost-effective, scalable security solutions through effective leverage of IBM protection platform.

The ISS approach to HIPAA security requirements

In order to streamline security and help meet the administrative, technical and physical safeguards of HIPAA compliance, IBM ISS has developed a five-step process that covers the complete security management lifecycle, including phases for assessment, design, deployment, management and education. This process is used to help identify and analyze gaps between current state and HIPAA requirements. It is then used to help design and implement that help close those gaps and ensure that the gaps remain closed.

The following phases are part of the five-step process:

**Phase 1.** Assessment
Meet HIPAA administrative safeguards
Action: Assess current level of information security.
Result: Help analyze gap between current information security levels and HIPAA requirements.

**Phase 2.** Design
Meet HIPAA administrative safeguards
Action: Design and document policies, processes and solutions to strengthen protection.
Result: Helps create gap closure plan.

**Phase 3.** Deployment
Meet HIPAA technical and physical safeguards
Action: Deploy protection technology and services.
Result: Help execute gap closure plan.

**Phase 4.** Management and support
Help meet HIPAA administrative safeguards
Action: Manage security program to serve business goals.
Result: Helps gaps remain closed and help prevent new gaps.

**Phase 5.** Education
Meet HIPAA administrative safeguards
Action: Educate organization on security Best practices and best-of-breed technology.
Result: Helps employees understand HIPAA responsibilities.

Health Insurance Portability and Accountability Act security requirements made simple

HIPAA mandates all healthcare organizations effectively meet administrative, technical and physical safeguards.
IBM ISS solutions for achieving HIPAA compliance

Section One: Administrative safeguards

In general, the administrative safeguards of HIPAA compliance require documented policies and procedures for day-to-day operations, managing the conduct of employees with personal health information (PHI) and managing the selection, development and use of security controls.

IBM ISS is uniquely able to help provide comprehensive compliance with the administrative safeguards with the research and consulting offerings of the Professional Security Services group. This group provides industry-leading methodologies to help assess an organization’s risk and security infrastructure, as well as design a successful implementation plan to achieve HIPAA compliance.

### Requirement | Description | IBM ISS program phase | IBM ISS solutions to achieve HIPAA compliance
---|---|---|---
Security management process 164.308(a)(1) | Implement policies and procedures to prevent, detect, contain and correct security violations. (A) Risk analysis (required). (B) Risk management (required). (C) Sanction policy (required). (D) Information system activity review (required). | Assess | Professional Security Services:  
• IBM Information Security Assessment  
• IBM Application Security Assessment  
• IBM Policy Development  
• IBM Penetration Testing  
• IBM Vulnerability Management Service (VMS)

Assigned security responsibilities 164.308(a)(2) | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. | Design | Professional Security Services:  
• Policy Development

Workforce security 164.308(a)(3) | Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. (A) Authorization and/or supervision (addressable). (B) Workforce clearance procedure (addressable). (C) Termination procedures (addressable). | Design | Professional Security Services:  
• Policy Development

Information access management 164.308(a)(4) | Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. (A) Isolating health care clearinghouse functions (required). (B) Access authorization (addressable). (C) Access establishment and modification (addressable). | Design | Professional Security Services:  
• Policy Development  
• Best practices  
• Documentation  
• Vulnerability Management Service

Security awareness and training 164.308(a)(5) | Implement a security awareness and training program for all members of its workforce (including management). (A) Security reminders (addressable). (B) Protection from malicious software (addressable). (C) Log-in monitoring (addressable). (D) Password management (addressable). | Educate | IBM Internet Security Systems  
Education Services  
Professional Security Services:  
• Policy Development

Security incident procedures 164.308(a)(6) | Implement policies and procedures to address security incidents. (A) Response and reporting (required). | Design | Professional Security Services:  
• Vulnerability Management Service (VMS)  
• Policy Development  
• IBM Emergency Response Services  
• IBM Protection Platform  
• IBM SiteProtector™ system  
Managed Security Services:  
• Ongoing monitoring and reporting

Contingency plan 164.308(a)(7) | Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain electronic protected health information. (A) Data backup plan (required). (B) Disaster recovery plan (required). (C) Emergency mode operation plan (required). (D) Testing and revision procedures (addressable). (E) Applications and data criticality analysis (addressable). | Manage and support | Professional Security Services:  
• Ongoing monitoring and reporting

Audit and Assessment Tools:  
IBM Protection Platform;  
Audit and Assessment Tools:  
• IBM Internet Scanner® Software  
• IBM System Scanner™ vulnerability assessment application  
Managed Protection Services:  
• Ongoing monitoring and reporting

Ongoing monitoring and reporting

Business associate contracts and other arrangement 164.308(b)(11) | Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart. | Manage and support | Professional Security Services:  
• Information Security Assessment  
• Penetration Testing  
IBM Protection Platform:  
Audit and Assessment Tools:  
• IBM Internet Scanner® Software  
• IBM System Scanner™ vulnerability assessment application  
Managed Protection Services:  
• Ongoing monitoring and reporting

IBM ISS has demonstrated proven success helping organizations quickly and simply achieve HIPAA security mandates.

Continued on next page
IBM ISS solutions for achieving HIPAA compliance

Section Two: Technical safeguards
The technical safeguards category is made up of several security measures that specify how to use technology to protect electronic personal health information (EPHI), particularly controlling access to it. IBM ISS enables your organization to achieve HIPAA compliance by delivering unparalleled detection, prevention and response to online threats with best-of-breed technology.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>IBM ISS solutions to achieve HIPAA compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control 164.312 (a)(1)</td>
<td>Implement technical policies and procedures for electronic information systems that maintain electronic protected health information (EPHI) to allow access only to those persons or software programs that have been granted access rights as specified in Administrative Standards section. (A) Unique user identification (addressable). (B) Emergency access procedure (required). (C) Automatic logoff (addressable). (D) Encryption and decryption (addressable).</td>
<td>Professional Security Services: Policy Development. Deploy.</td>
</tr>
<tr>
<td>Audit control 164.312 (b)</td>
<td>Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</td>
<td></td>
</tr>
<tr>
<td>Integrity 164.312 (c)(1)</td>
<td>Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. Implementation specification: Mechanism to authenticate electronic protected health information (addressable). Implement electronic mechanisms to combine individual electronic protected health information in a manner that ensures that only the person authorized to use the information has been altered or destroyed in an unauthorized manner.</td>
<td></td>
</tr>
<tr>
<td>Person or entity authentication 164.312 (d)</td>
<td>Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.</td>
<td></td>
</tr>
<tr>
<td>Transmission security 164.312 (a)(1)</td>
<td>Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. (A) Integrity controls (addressable). (B) Encryption (addressable).</td>
<td></td>
</tr>
</tbody>
</table>

Section Three: Physical safeguards
The physical safeguards are a series of security measures meant to protect the environment of the electronic information systems, as well as the related buildings and equipment from natural and environmental hazards and unauthorized intrusion. These measures include both administrative policies and physical controls.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>IBM ISS solutions to achieve HIPAA compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility access controls 164.308(a)(1)</td>
<td>Implement policies and procedures to limit physical access to the electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed: (A) Contingency operations (addressable). (B) Facility security plan (addressable). (C) Access control and validation procedures (addressable). (D) Maintenance records (addressable).</td>
<td>Professional Security Services: Policy Development. Deploy.</td>
</tr>
<tr>
<td>Workstation use 164.310 (b)</td>
<td>Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed and the physical attributes of the environment of a specific workstation or class of workstation that can access electronic protected health information.</td>
<td></td>
</tr>
<tr>
<td>Workstation security 164.310 (c)</td>
<td>Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.</td>
<td></td>
</tr>
<tr>
<td>Device and media controls 164.308(d)(1)</td>
<td>Implement policies and procedures that govern the receipt and removal of hardwares and electronic media that contain EPHI in and out of a facility, and the movement of these items within the facility: (A) Disposal (required). (B) Media re-use (required). (C) Accountability (addressable). (D) Data backup and storage (addressable).</td>
<td>Professional Security Services: Policy Development. Deploy.</td>
</tr>
</tbody>
</table>

IBM ISS enables your organization to achieve HIPAA compliance by delivering unparalleled detection, prevention and response to online threats.
Get started today
IBM ISS offers healthcare organizations a single source for guidance, expertise and technology that addresses HIPAA security requirements. By partnering with IBM ISS, organizations benefit from the best security intelligence in the world, freeing resources to focus on other areas of HIPAA compliance.

About IBM Internet Security Systems
IBM ISS is the trusted security expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, IBM ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. IBM ISS products and services are based on the proactive security intelligence conducted by the IBM Internet Security Systems X-Force® research and development team – a world authority in vulnerability and threat research. For more information, visit ibm.com/services/us/iss or call 1 800 776-2362.