



IBM Internet Security Systems for achieving Health Insurance Portability and Accountability Act compliance

Section One: Administrative safeguards

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

IBM Internet Security Systems™ (ISS) is uniquely able to provide comprehensive compliance with the administrative safeguards with the research and consulting offerings provided by IBM Professional Security Services. This group provides industry-leading methodologies to help assess your 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: <ul style="list-style-type: none">• <i>IBM Information Security Assessment</i>• <i>IBM Application Security Assessment</i>• <i>IBM Policy Development</i>• <i>IBM Penetration Testing</i>• <i>IBM Vulnerability Management Service (VMS)</i>
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: <ul style="list-style-type: none">• <i>Policy Development</i>
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: <ul style="list-style-type: none">• <i>Policy Development</i>• <i>Best practices</i>• <i>Documentation</i>

IBM ISS Solutions for achieving HIPAA compliance

Requirement	Description	IBM ISS program phase	IBM ISS solutions to achieve HIPAA compliance
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: <ul style="list-style-type: none"> • <i>Policy Development</i> • <i>Best practices</i> • <i>Documentation</i> • <i>Vulnerability Management Service</i>
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: <ul style="list-style-type: none"> • <i>Policy Development (Security awareness program development)</i>
Security incident procedures 164.308 (a) (6)	Implement policies and procedures to address security incidents. (A) Response and Reporting (required).	Design	Professional Security Services: <ul style="list-style-type: none"> • <i>Vulnerability Management Service</i> • <i>Policy Development</i> • <i>IBM Emergency Response Services</i> IBM Internet Security Systems protection platform: <ul style="list-style-type: none"> • <i>IBM SiteProtector™ system</i> Managed Security Services: <ul style="list-style-type: none"> • <i>IBM Managed Protection Services</i> • <i>Ongoing monitoring and reporting</i>
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: <ul style="list-style-type: none"> • <i>Policy Development</i> • <i>Emergency Response Services</i> IBM Managed Protection Services (MPS): <ul style="list-style-type: none"> • <i>Ongoing monitoring and reporting</i>
Evaluation 164.308 (a) (8)	Perform a periodic technical and nontechnical 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: <ul style="list-style-type: none"> • <i>IBM Information Security Assessment</i> • <i>IBM Penetration Testing</i> IBM Protection Platform: <ul style="list-style-type: none"> • <i>IBM Internet Scanner® Software</i> • <i>IBM System Scanner™ vulnerability assessment application</i> Managed Protection Services: <ul style="list-style-type: none"> • <i>Ongoing monitoring and reporting</i>
Business associate contracts and other arrangement 164.308 (b) (1)	A covered entity may permit a business associate to create, receive, maintain or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate will appropriately safeguard the information.	Design	Professional Security Services: <ul style="list-style-type: none"> • <i>Policy Development</i> • <i>IBM Information Security Assessment</i>

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 protected health information (EPHI), particularly controlling access to it. The specific standards of the technical safeguards are to use technology to protect EPHI, particularly controlling access to it.

IBM ISS enables your organization to achieve HIPAA compliance by The technical safeguards category is made up of several security delivering unparalleled detection, prevention and response to measures that specify how to use technology to protect EPHI, online threats with best-of-breed technology.

Requirement	Description	IBM ISS program phase	IBM ISS solutions to achieve HIPAA compliance
Access control 164.312 (a) (1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information 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 (required). (B) Emergency access procedure (required). (C) Automatic logoff (addressable). (D) Encryption and decryption (addressable).	Deploy	Professional Security Services: <ul style="list-style-type: none"> • <i>Policy Development</i> IBM protection platform: <ul style="list-style-type: none"> • <i>Proventia® Network Intrusion Prevention System</i> • <i>Proventia Server Intrusion Prevention System</i> • <i>Proventia Desktop Endpoint Security</i> • <i>IBM RealSecure® Network</i> • <i>IBM RealSecure Desktop</i> • <i>IBM RealSecure Server Sensor</i>
Audit control 164.312 (b)	Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Deploy	IBM protection platform: <ul style="list-style-type: none"> • <i>RealSecure Server Sensor</i> • <i>System Scanner vulnerability assessment application</i>
Integrity 164.312 (c) 1	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 corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Deploy	Professional Security Services: <ul style="list-style-type: none"> • <i>Policy Development</i>
Person or entity authorization 164.312 (d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Deploy	IBM protection platform: <ul style="list-style-type: none"> • <i>RealSecure Desktop</i> • <i>Dual authentication</i>
Transmission security 164.312 (e) (1)	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).	Deploy	IBM protection platform: <ul style="list-style-type: none"> • <i>IBM Proventia® Server Intrusion Prevention System</i>

IBM ISS Solutions for achieving HIPAA compliance

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.

Requirement	Description	IBM ISS program phase	IBM ISS solutions to achieve HIPAA compliance
Facility access controls 164.308 (a) (1)	Implement policies and procedures to limit physical access to its 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).	Deploy	Professional Security Services: <ul style="list-style-type: none"> • <i>Policy Development</i>
Workstation use 164.310 (b)	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 surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Design	Professional Security Services: <ul style="list-style-type: none"> • <i>Policy Development</i>
Workforce security 164.308 (c)	Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.	Deploy	Professional Security Services: <ul style="list-style-type: none"> • <i>Policy Development</i>
Device and media 164.308 (d) (1)	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into (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).	Design	Professional Security Services: <ul style="list-style-type: none"> • <i>Policy Development</i>



© Copyright IBM Corporation 2007

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.
10-07
All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Internet Security Systems and X-Force are trademarks or registered trademarks of IBM Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.