



Achieving a Clean Bill of Health in HIPAA Compliance with Check Point Solutions

Contents

Executive summary	3
Overview of HIPAA and the healthcare environment	4
The HIPAA security challenge.....	7
A healthy compliance approach.....	9
Check Point solutions mapped to HIPAA	10
Conclusion	23

Executive summary

Healthcare organizations face both opportunities and challenges from today's complex, interconnected environment in which electronic information is collected and exchanged at an ever-increasing rate. While electronic information exchange has the potential to deliver profound benefits, it also increases the exposure of sensitive information. Adding to the challenge are new technologies and a heightened demand by physicians, healthcare workers, and patients for flexible access to health information. The Health Insurance Portability and Accountability Act (HIPAA) security standards are designed to ensure that healthcare organizations maintain the confidentiality, integrity, and availability of sensitive patient information.

These healthcare organizations must comply with HIPAA security standards that are vague and that offer little guidance about how to achieve compliance. In responding to HIPAA requirements, healthcare organizations must seek solutions that are ongoing and repeatable, addressing multiple HIPAA requirements and reducing integration challenges. These organizations can use technology to help build ongoing, repeatable solutions for compliance.

Check Point Software Technologies, a worldwide leader in trusted network security, offers a suite of solutions that support healthcare organizations in achieving healthy compliance with HIPAA security standards. These solutions are comprehensive and integrated, providing a solid base for HIPAA compliance while also supporting requirements common to other security regulations. In addition to enabling compliance, Check Point solutions deliver fundamental business value to healthcare organizations by ensuring business continuity, enabling safe business communications, and protecting and enhancing the ongoing trust of patients and partners.

Overview of HIPAA and the healthcare environment

Today's interconnected, digital world presents both challenges and opportunities to the modern healthcare enterprise. In unprecedented fashion, healthcare organizations are collecting, processing, managing, and sharing electronic information—including sensitive patient information—among providers, payers, and patients. This has the potential to increase operational efficiencies, lower costs, and improve the delivery of care. Many different parties can now touch patient information quickly and efficiently. With increased use of Web, wireless, and other network technologies, healthcare providers, payers, and patients can now access information remotely, using an array of endpoint devices including laptop computers, personal digital assistants, cell phones, and Internet kiosks.

However, these benefits come with a risk. Along with the increase in information sharing, openness, new technologies, and flexible access comes an increased vulnerability—an exposure to threats that can compromise the information being shared, much of which is confidential. The Health Insurance Portability and Accountability (HIPAA) Security Rule is one response to this vulnerability.

About the Health Insurance Portability and Accountability Act of 1996

Title I of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects workers and their families when they change or lose jobs. Title II, Administrative Simplification, was designed to encourage the use of electronic data interchange to streamline and simplify health insurance claims and to reduce fraud and abuse. More recently, HIPAA requirements were added to protect the privacy and security of patient health information. The HIPAA Security Rule—finalized on Feb. 20, 2003, and the subject of this white paper—specifically safeguards the confidentiality, integrity, and availability of electronic protected health information (EPHI). Healthcare organizations have spent considerable effort in addressing this set of recent requirements.

HIPAA applies to all healthcare providers (hospitals, physicians), payers (insurance companies, self-insured employers), and healthcare information clearinghouses. Most HIPAA rules are now mandatory. The standard for a National Provider Identifier became mandatory on a rolling schedule in May 2007. Enforcement is administered by the Centers for Medicare and Medicaid Services (CMS), a federal agency within the United States (U.S.) Department of Health & Human Services. Healthcare organizations that fail to comply face potential administrative actions, fines, and even criminal prosecution. Healthcare companies experiencing a breach in protection of sensitive information risk a loss of trust from patients and partners and damage to their reputations.

Despite the deadlines having come and gone, many organizations were found to be out of compliance, according to surveys conducted in 2006 by both the Health Information and Management Systems Society (HIMSS) and the American Health Information Management Association (AHIMA). According to these studies, as of winter 2006, about 55 percent of healthcare providers reported that they were compliant with security standards and 72 percent of payers were reportedly compliant. The HIMSS study also revealed that the percentage of payers reporting privacy breaches rose from 45 percent in July 2005 to 66 percent in January 2006.^{1,2} Healthcare organizations are pressing to comply with and to strengthen security controls going forward.

The HIPAA security standards comprise general requirements and three categories of safeguards: administrative, physical, and technical. These are summarized below.

HIPAA standards for the security of electronic health information – Final Security Rule, 2003

<p>General requirements (Section 164.306) – require entities to do the following:</p> <ul style="list-style-type: none"> • Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits • Protect against any reasonably anticipated threats or hazards to the security or integrity of such information • Protect against any reasonably anticipated uses or disclosures of such information that are not permitted • Ensure compliance by the workforce
<p>Administrative safeguards (Section 164.308) – require that entities implement policies and procedures to prevent, detect, contain, and correct security violations. This includes security management, workforce security, information access management, security awareness and training (including protection from malicious software), security incident handling, and contingency planning.</p>
<p>Physical safeguards (Section 164.310) – require the implementation of policies and procedures to limit physical access to electronic information systems and the facilities in which they are housed.</p>
<p>Technical safeguards (Section 164.312) – stipulate requirements for technical policies, procedures, and hardware/software mechanisms regarding access control, audit controls, integrity protection, authentication, and transmission security.</p>

At the same time that healthcare organizations are working to comply with HIPAA, many are engaged in efforts to comply with other regulations. Examples include the Sarbanes-Oxley Act of 2002, which contains information security requirements as part of overall governance mandates; California SB1386, which requires companies to publicly disclose when there’s been a breach in information security; and the Payment Card Industry standards affecting all businesses that process credit-card transactions. Despite these overlaps in requirements, different departments within an organization often manage these initiatives.

¹ The State of HIPAA Privacy and Security Compliance, American Health Information Management Association, April 2006.

² HIPAA Advisory: U.S. Healthcare Industry Compliance Survey Results: Winter 2006, HIMSS/Phoenix Health Systems.

Because of HIPAA and other prominent regulations, compliance is one of the primary drivers of IT spending. Hospital budgets for HIPAA compliance efforts in 2006 were generally consistent with HIPAA expenditures in 2005 according to U.S. Healthcare Industry HIPAA Compliance Survey Results—Winter 2006 (Figure 1).

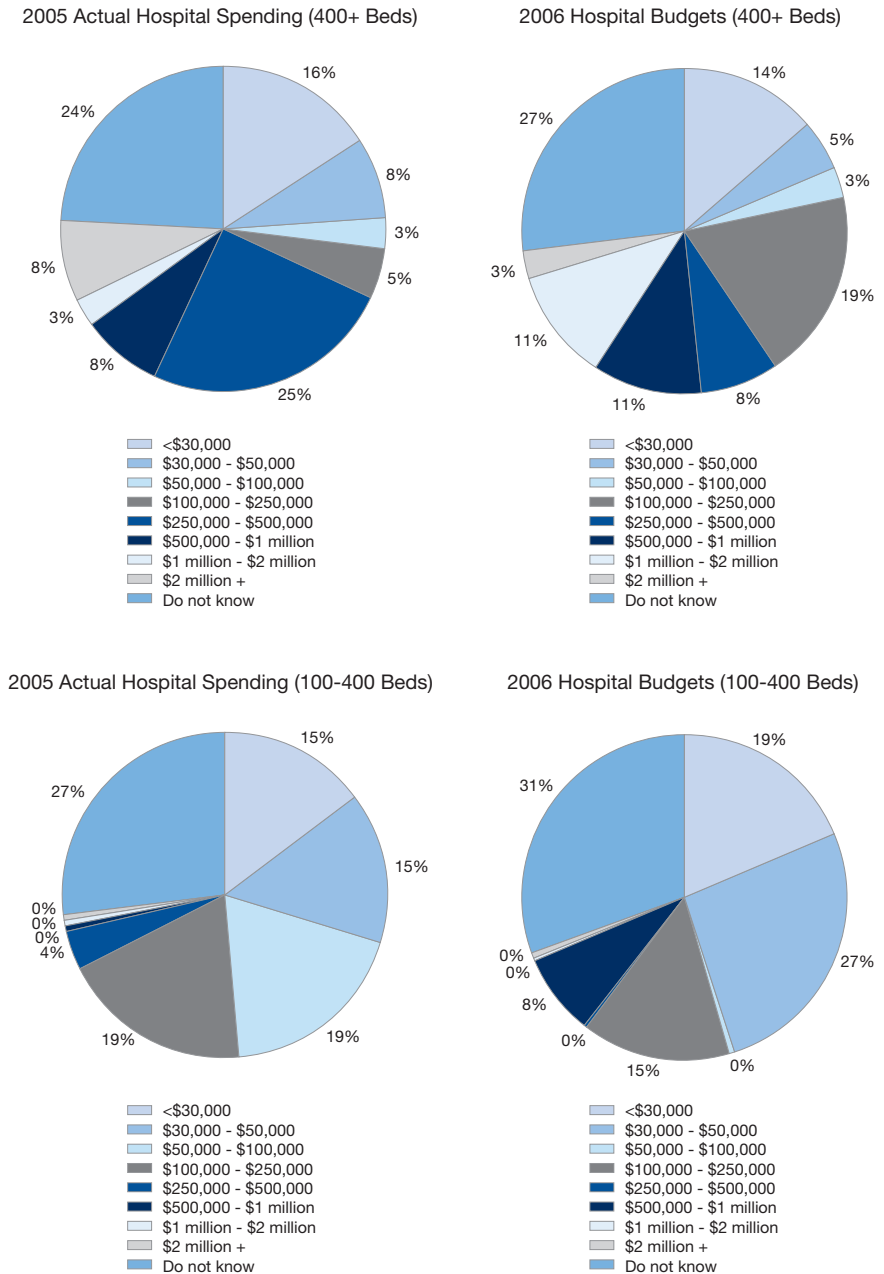


Figure 1: U.S. Healthcare Industry HIPAA Compliance Survey Results—Winter 2006

The HIPAA security challenge

Several forces contribute to the challenge of protecting health information: the extended nature of organizations and communications networks; increased collection, processing, and exchange of information; increased demand for physician, patient, and employee access to information; new technologies; and increasingly sophisticated cyber attacks and threats. When so many parties can touch information—and the networks on which the information is stored and transmitted—it becomes difficult for healthcare organizations to maintain appropriate protections.

For example, a physician may need to access medical records, order lab tests, and view results. Or a nurse may need to view electronic patient records and view but not order tests. Perhaps, a finance department employee may need to view patient financial data, a claims manager may need to approve claims, or an affiliated physician may need to submit claims and view selected patient records. And patients could require access, too. To be in compliance, healthcare organizations must tighten network security controls and increase scrutiny to ensure that only appropriate parties can access selected information and specific parts of the network.

The increased use of Web applications and remote access, which supports an increasingly mobile healthcare workforce, has become a target of sophisticated intrusions and malicious attacks. This raises the need for secure Web and remote access controls.

Another challenge faced by healthcare organizations is managing endpoint devices. With the expanded reach and variety of endpoint devices, it is difficult to maintain consistent controls. It is important to ensure that authorized users gain access only through endpoint devices that are up-to-date with antivirus software, anti-spyware, and other policy protections.

Increasingly complex and expansive communication networks have made it more difficult for security officers within healthcare organizations to gain an overall, comprehensive view of their security posture. Between the vast number of network and security devices to manage and vendor solutions that are not integrated, administrators often lack the ability to centrally monitor, manage, and report across a full range of security devices.

Medical devices used in hospitals and other healthcare facilities pose another security challenge. Once developed as proprietary systems, medical devices are now built on commercial operating systems connected to healthcare networks, exposing them to viruses, worms, and cyber attacks. The solution, as described by Forrester Research, lies in two key capabilities: a perimeter firewall with Stateful Inspection and the use of network isolation and intrusion prevention to monitor and prevent attacks.³

³ The Role of Network Intrusion Prevention in Protecting Medical Devices, Michael Rasmussen, Forrester Research, Dec. 7, 2004.

HIPAA security requirements do not provide much guidance

Like most other information security-related regulations, HIPAA security requirements are vague. They only describe what to do at a high level but provide no guidance on how to achieve compliance. The HIPAA Security Rule does not require specific technology solutions—security measures and technical solutions are provided in the rule only as examples. For instance, the rule includes requirements for preventing unauthorized access to resources on the network but does not mandate the use of firewalls. Although, firewalls are the recommended choice for meeting this requirement according to more detailed frameworks from the National Institute of Standards and Technology (NIST) and others. Thus, healthcare organizations face the challenge of translating high-level regulation requirements into actionable controls.

Adding to the confusion, HIPAA security requirements are stipulated either as required or addressable. In the latter case, it is up to the affected organization to assess "whether it is a reasonable and appropriate safeguard in the entity's environment." This involves analyzing the specification in reference to the likelihood of protecting the entity's EPHI from reasonably anticipated threats and hazards.⁴ An organization must be prepared to defend and document why it has chosen not to anticipate an addressable requirement.

Facing limited guidance, tight time frames, and constrained resources, some healthcare organizations are experiencing more success than their counterparts when it comes to putting in place ongoing, repeatable solutions for compliance. Even fewer are taking a holistic look across multiple regulatory compliance initiatives.

⁴ Security 101 for Covered Entities, HIPAA Security Series, Department of Health & Human Services, November 2004.

A healthy compliance approach

The challenges notwithstanding, healthcare organizations can take strong, appropriate measures to comply with HIPAA — measures that can lead to ongoing HIPAA compliance, support multiple regulations, and deliver additional business value. Conversely, a mindset of doing the minimum will leave organizations in pain: from fragmented and inefficient solutions, continued high operational risk, failure to reap business benefits from compliance activities, higher risk of noncompliance, and increased scrutiny if regulators do come calling.

Healthcare organizations should consider the following as they build and strengthen their compliance with HIPAA:

1. Build a strong base of compliance solutions with which the organization can grow. There will be a need for changing and adding capabilities over time. No single vendor solution will meet all HIPAA security requirements. It is imperative to choose solutions that are integrated and address multiple HIPAA requirements
2. Where possible, take a holistic look at compliance. Implement solutions that address core security capabilities to comply with other regulations. Examples of core security functionality include access and authorization controls, use of private networks and firewalls, security incident monitoring and detection across multiple devices, centralized management and reporting, malicious software protection, and use of encryption
3. Apply technology as a means of instituting repeatable processes. Automation in compliance has a lower total cost of ownership and is less prone to error, thus, lowering operational risk in the process. Security technology solutions serve as a way of translating high-level regulation requirements into actionable controls
4. Follow a due-care approach, using security solutions that lead in classes and established frameworks. Begin with HIPAA standards. For more guidance, apply the recommended security framework of NIST or others
5. Evaluate and consider solutions with an aim to deliver fundamental business value and create business differentiation. For healthcare organizations, this includes increasing operational efficiencies, reducing costs, ensuring business continuity, protecting trust, and improving the overall quality of care and patient safety

Check Point solutions mapped to HIPAA

As shown in the following table, Check Point solutions support compliance with many HIPAA administrative and technical safeguards. Check Point provides a broad set of security solutions that form a strong foundation for complying with any information security-related regulation. Check Point, together with its Open Platform for Security (OPSEC™) partners, provides customers with comprehensive, integrated security solutions allowing you to establish a firm base from which to build and grow compliance. Please see the individual product descriptions at the end of this document to find out how they can help achieve compliance.

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.308(a)(1)(ii)(B)	<p>Risk management (required)</p> <p>Implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level.</p> <p>Reasonable and appropriate refers to ensuring the confidentiality, integrity, and availability of all electronic protected health information (EPHI), providing protection against reasonably anticipated threats and protecting against reasonably anticipated uses of EPHI that are not permitted.</p>	<p>Application Intelligence™, Web Intelligence™, and patented Stateful Inspection are core technologies used across all Check Point solutions, including VPN-1®, InterSpect™, Connectra™, and Check Point Endpoint Security, to deliver network- and application-level firewall and intrusion prevention. Check Point solutions provide logical separation of security for network elements and mitigate the risks of malicious attacks on an organization's perimeter, internal, Web, or endpoint infrastructure.</p> <p>Check Point solutions ensure a consistent and effective perimeter, internal, Web, and endpoint security policy through a centralized management infrastructure. VPN-1, InterSpect, and Connectra can be managed under a single SmartCenter™ management console.</p> <p>SmartDefense™ Services provide real-time security updates for Check Point products and alert customers to new vulnerabilities and configuration policies, as well as provide information on possible risks to their networks and, as such, to their EPHI.</p>

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.308(a)(1)(ii)(D)	<p>Information system activity review (required)</p> <p>Implement procedures to regularly review information system activity, like audit logs, access reports, and security incident tracking reports.</p>	<p>SmartCenter and Eventia™ Suite— Eventia Reporter™ and Eventia Analyzer™—centralize logging, updating, monitoring, and reporting of system events and activity, enabling enterprises to gain a holistic picture of their security and network activity trends. The consistent presentation of data across the enterprise enables more effective data collection, analysis, and response.</p> <p>Eventia Suite collects, audits, correlates, and reports on logs and event activity across all Check Point products and across a diverse range of third-party products. Eventia Reporter gathers information to report on cross-product attacks, blocked traffic, login activity, and network activity.</p> <p>Eventia Reporter endpoint security reports include centralized reporting of Check Point Endpoint Security data on compliance violations, firewall events, blocked programs, Check Point Endpoint Security MailSafe™ events, spyware, Malicious Code Protector outcomes, and client errors. Eventia Reporter also provides reports on antivirus activity, Connectra, InterSpect, and VPN-1 Power VSX log reports.</p> <p>Eventia Suite enables enterprises to build audit trails of user access to data, administrator actions, invalid logical access attempts, and more. Eventia Analyzer supports the initialization of audit logs, secure access to audit information, and allows for creation and deletion of system-level objects. In addition, Eventia Analyzer provides alerts when the audit logs are initialized and when system objects are created and deleted.</p> <p>Check Point user authentication and logging features allow customers to implement audit trails to reconstruct and analyze system events.</p>

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
<p>§ 164.308(a)(3)(ii)(A)</p> <p>§ 164.308(a)(4)(ii)(B)</p> <p>§ 164.308(a)(4)(ii)(C)</p>	<p>§ 164.308(a)(3)(ii)(A) <i>Authorization and/or supervision (addressable)</i></p> <p>Implement procedures for the authorization and/or supervision of staff who work with EPHI or in locations where it might be accessed.</p> <p>§ 164.308(a)(4)(ii)(B) <i>Access authorization (addressable)</i></p> <p>Implement policies and procedures for granting access to EPHI through a workstation, transaction, program, process, or other mechanism.</p> <p>§ 164.308(a)(4)(ii)(C) <i>Access establishment and modification (addressable)</i></p> <p>Implement policies and procedures for reviewing and modifying user access privileges.</p>	<p>Check Point perimeter, internal, Web, and endpoint solutions allow for the creation of granular access and authorization rules. VPN-1 and InterSpect enforce access policies at the perimeter and on the internal network. Connectra and VPN-1 enforce access policies when providing remote access to users outside the perimeter. Check Point Endpoint Security uses desktop firewall rules and network zones to limit PC access to network resources and segments. These access policies define what resources an individual, group, or department is authorized to view.</p> <p>Check Point products can segment and provide EPHI security in a variety of deployments. VPN-1 can establish a secure network perimeter around EPHI, separating it from an external network. InterSpect allows internal network segmenting, or zoning, to provide EPHI security inside a network. VPN-1 and Connectra provide access control and authorization for external users who need remote access to EPHI. And Check Point Endpoint Security provides access control security for endpoint systems that contain or attempt access to EPHI.</p> <p>For large enterprises and managed service providers, Check Point provides granular administrative controls via Provider-1® management solutions so that different IT teams or administrators can be given different levels of access based on their responsibilities within the organization.</p>

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
<p>§ 164.308(a)(3)(ii)(B)</p> <p>§ 164.308(a)(3)(ii)(C)</p>	<p>§ 164.308(a)(3)(ii)(B) <i>Workforce clearance procedure (addressable)</i></p> <p>Implement procedures to determine that access by staff to EPHI is appropriate.</p> <p>§ 164.308(a)(3)(ii)(C) <i>Termination procedures (addressable)</i></p> <p>Implement procedures for terminating access to EPHI when employees terminate employment.</p>	<p>Check Point management tools allow administrators to create policies, including the mapping and assignment of groups (of users and endpoints) to resources. All Check Point products can log and report user access across Check Point gateways as well as log and report administrator changes on Check Point systems. Organizations can view this data in SmartViewTracker™ and in reports from Eventia Reporter.</p> <p>Authentication is an essential part of all Check Point solutions, including Check Point VPN solutions, as well as user authentication for VPN-1. VPN-1 supports multiple databases for authentication, including an internal database, Microsoft Active Directory, and OPSEC-certified LDAP and RADIUS databases.</p> <p>Check Point VARs, SIs, and business partners can provide consulting services to help an organization define an ID program that can assign users with unique IDs for use with Check Point solutions.</p>

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.308(a)(4)(ii)(A)	<p>§ 164.308(a)(4)(ii)(A) <i>Isolating healthcare clearinghouse functions (required)</i></p> <p>Implement procedures that protect EPHI of the clearinghouse from unauthorized access by the larger organization (in cases where the clearinghouse is a part of a larger organization).</p>	<p>A core Check Point capability, Check Point perimeter, internal, Web, and endpoint solutions can cordon off a healthcare clearinghouse (or other department or function) from other parts of the business. Check Point solutions can segregate the healthcare clearinghouse within the same physical or virtual network.</p> <p>Check Point products can segment and enforce security access policy to clearinghouse functions and EPHI in a variety of deployments. VPN-1 can establish a secure network perimeter around EPHI, separating it from an external network. InterSpect allows internal network segmenting, or zoning, to provide security for EPHI inside a network. VPN-1 and Connectra provide access control and security for external users who need remote access to EPHI. And Check Point Endpoint Security provides access control security for endpoint systems that contain or access EPHI.</p> <p>Check Point also provides the ability to segregate the administration and management of security policies and to log data of a healthcare clearinghouse from other departments or businesses within the larger organization.</p>

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.308(a)(4)(ii)(A)	<p>§ 164.308(a)(5)(ii)(A) <i>Security reminders (addressable)</i></p> <p>Implement periodic security updates.</p>	<p>Check Point perimeter, internal, Web, and endpoint security solutions allow administrators to pass appropriate messages and reminders to users, such as to update their antivirus or other software. Check Point Endpoint Security automatically checks the level of compliance of user desktops and can push out reminders or even required software updates.</p> <p>Connectra, InterSpect, and VPN-1 allow administrators to inform users when they are out of security compliance, when their compliance is out-of-date, as well as which remediation steps are required to come into compliance. SmartDefense™ Services provide updates and advisories, including code updates, best practices on configuration management, warnings of new viruses, and policy recommendations, to administrators of Check Point perimeter, internal, Web, and endpoint solutions.</p>
§ 164.308(a)(5)(ii)(B)	<p>§ 164.308(a)(5)(ii)(B) <i>Protection from malicious software (addressable)</i></p> <p>Implement procedures for guarding against, detecting, and reporting malicious software.</p>	<p>Application Intelligence™ and Web Intelligence™ are core technologies used across many Check Point products, including VPN-1, InterSpect, Connectra, and Check Point Endpoint Security, designed to address threats from malicious software, such as worms and spyware. VPN-1 and Connectra protect against malicious software entering a network. InterSpect segments an internal network and protects it from malicious software introduced inside the network. Check Point Endpoint Security includes antivirus and anti-spyware capabilities that protect endpoint PCs from infection. Check Point Endpoint Security protects endpoints and the networks they connect to from malicious software.</p> <p>Check Point security information and event management tool, Eventia Analyzer, analyzes and correlates data to detect previously undetected threats that arise from more than one source.</p>

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.308(a)(5)(ii)(C)	<p>§ 164.308(a)(5)(ii)(C) <i>Login monitoring (addressable)</i></p> <p>Implement procedures for monitoring login attempts and reporting discrepancies.</p>	<p>Check Point solutions designed to provide remote access, including VPN-1 and Connectra, record login attempts. In addition, these logs can be sent to management tools such as Eventia Analyzer and SmartView Monitor™ for real-time monitoring and response. Eventia Analyzer monitors login attempts across a broad range of heterogeneous security and network devices. It can be set to identify multiple unsuccessful login attempts, trigger alerts, and block further connection attempts.</p> <p>SmartViewTracker and SmartView Monitor allow security administrators to view logging activity for all Check Point gateways. Eventia Reporter provides historical reports of logging activity.</p>
§ 164.308(a)(5)(ii)(D)	<p>§ 164.308(a)(5)(ii)(D) <i>Password management (addressable)</i></p> <p>Implement procedures for creating, changing, and safeguarding passwords.</p>	<p>For example, VPN-1, forces customers to change the default password during the initial installation. In addition, it checks to ensure that “weak” passwords are not allowed, thwarting hackers with access to common information.</p> <p>As required in the sub-requirements to 2.1, VPN-1 UTM Edge™ W includes Wi-Fi Protected Access (WPA) technology for encryption and authentication of wireless traffic.</p> <p>Through centralized management and administration, VPN-1 solutions allow enterprises to mandate passwords, keys, and other settings and propagate these settings down to the remote devices deployed across the organization, e.g., in distributed sales offices.</p> <p>Check Point VARs, SIs, and business partners can provide consulting services to help implement Check Point solutions in an organization’s architecture to ensure these security checks are applied in the relevant sections of the network as required to achieve the goals of this requirement.</p>

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.308(a)(6)(ii)	<p>§ 164.308(a)(6)(ii) <i>Security incident response and reporting (required)</i></p> <p>Implement policies and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects, and document incidents and outcomes.</p>	<p>SmartDefense and Web Intelligence technologies perform intrusion prevention as part of Connectra, Check Point Endpoint Security, and VPN-1 products. SmartDefense Services allow enterprises to keep intrusion prevention engines updated.</p> <p>Eventia Analyzer provides comprehensive support for the identification, handling, and reporting of security incidents. It analyzes log data in near real-time from Check Point solutions and commonly used security devices to identify significant threats across the network. Upon the detection of a security event, Eventia Analyzer can be preset to generate alerts or reports or to take appropriate action to mitigate the detected threat.</p> <p>Eventia Reporter enables real-time, historical, and trend reporting of security events.</p> <p>IPS-1 is a dedicated intrusion prevention system that delivers mission-critical protection and granular forensic analysis capabilities and flexible deployment.</p>

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.308(a)(7)(ii)(B)	<p>§ 164.308(a)(7)(ii)(B) <i>Disaster recovery plan (required)</i></p> <p>Implement procedures to restore any loss of data.</p>	<p>Check Point solutions, including VPN-1, InterSpect, Check Point Endpoint Security, and Connectra provide critical high availability and clustering capabilities to mitigate risks from hardware failure. In addition, VPN-1 gateways enable an organization to utilize WAN connections from multiple Internet service providers (ISPs) to mitigate and recover from ISP disasters.</p> <p>All Check Point gateways enable you to save and archive configuration data—including device configuration, user policies, and activity—on a regular basis. This information can be stored locally or remotely and used to restore configuration and service to Check Point products.</p> <p>Check Point management architecture allows users to deploy a second SmartCenter server for automatic failover in an emergency. The inactive server can be activated automatically without losing any data. The servers are synchronized in real-time so that there is no data loss, affording continuous access to critical security policy and log data.</p>
§ 164.308(a)(7)(ii)(C)	<p>§ 164.308(a)(7)(ii)(C) <i>Emergency mode operation plan (required)</i></p> <p>Implement procedures to enable continuation of critical business processes for protection of EPHI while in emergency mode.</p>	<p>In the case of disaster affecting an organization's physical locations, Check Point remote access solutions, VPN-1 and Connectra, enable network access from external locations. This enables continued secure access to EPHI in an emergency.</p> <p>Check Point provides the ability to track the access activity to different areas during emergencies and properly audit it upon return to normal conditions. Check Point provides the ability to track configuration and policy changes and enables users to go back to an earlier version after an emergency is resolved.</p>

Administrative Safeguards HIPAA Security Rule 164.308		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.308(b)(1)	<p>§ 164.308(b)(1) <i>Business associate contracts and other arrangements</i></p> <p>A covered entity may permit a business associate to create, receive, maintain, or transmit EPHI only if the covered entity obtains satisfactory assurances that the business associate will safeguard the information.</p>	<p>VPN-1 solutions can help demonstrate security controls around the business associate network and secure transmission of EPHI. InterSpect and Check Point Endpoint Security can help demonstrate internal safeguards for EPHI inside a business associate network. Check Point Web solutions, including Connectra, can help demonstrate safeguards when sharing, receiving, or transmitting information over the Web.</p> <p>Eventia Reporter provides automated reports of security and network activity that can be easily generated for business associates receiving, maintaining, and transmitting EPHI.</p>

Technical Safeguards HIPAA Security Rule 164.312		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.312(a)(2)(i)	<p>§ 164.312(a)(2)(i) <i>Unique user identification (required)</i></p> <p>Assign unique names/ numbers for identifying and tracking user identities.</p>	<p>A core functionality within Check Point secure remote access solutions VPN-1 and Connectra is the capability of administrators to assign and monitor users by unique user IDs. Check Point products support the creation of unique user IDs through an internal database as well as supporting unique user IDs created in external databases. Through the Check Point OPSEC program, customers have access to multiple authentication and identification mechanisms including digital certificates, biometrics, and tokens.</p> <p>Check Point unified management supports the tracking of user activities across Check Point perimeter, internal, Web, and endpoint solutions by users assigned unique IDs.</p>
§ 164.312(a)(2)(ii)	<p>§ 164.312(a)(2)(ii) <i>Emergency access procedure (required)</i></p> <p>Implement procedures for obtaining necessary EPHI during an emergency.</p>	<p>Check Point remote access solutions, VPN-1, Check Point Endpoint Security, and Connectra, enable anywhere, anytime access to EPHI in the event of an emergency. This includes the provision of emergency passwords.</p>

Technical Safeguards HIPAA Security Rule 164.312		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.312(a)(2)(iii)	<p>§ 164.312(a)(2)(iii) <i>Automatic logoff (addressable)</i></p> <p>Implement procedures to terminate an electronic session after a predetermined time of inactivity.</p>	<p>Check Point remote access solutions, VPN-1 and Connectra, require user reauthentication following a period of inactivity. This ensures continued access to EPHI for active sessions while terminating inactive sessions.</p>
§ 164.312(a)(2)(iv)	<p>§ 164.312(a)(2)(iv) <i>Encryption and decryption (addressable)</i></p> <p>Implement a mechanism to encrypt and decrypt EPHI.</p>	<p>Pointsec PC delivers the highest level of data security by providing a strong, full-disk encryption solution for PCs and laptops as well as access control. Pointsec PC enables the secure exchange of sensitive data by ensuring the integrity and authenticity of data.</p> <p>Check Point remote access solutions, VPN-1 and Connectra, provide strong encryption for data during transmission over open networks using standards-based encryption protocols. VPN-1 supports SSL- and IPSec-encrypted communication protocols. Connectra supports SSL- and TLS-encrypted communication protocols. In addition, both products support the MD5 and SHA-1 protocols to ensure the integrity of secure transmissions involving cardholder data.</p> <p>VPN-1 UTM Edge W, which provides Wi-Fi access as part of the solution, employs IPSec-over-WLAN encryption and enables the regular rotation of WEP keys. It supplements WEP, WPA, and WPA with inspection by Check Point firewall, intrusion prevention, and antivirus technologies. Users who use IPSec-over-WLAN rather than WEP can be granted higher access rights, as well.</p> <p>Check Point VARs, SIs, and business partners can provide consulting services to deploy Check Point solutions within an organization to enable the secure exchange of data.</p>

Technical Safeguards HIPAA Security Rule 164.312		
HIPAA Standard	Implementation specification (summary)	Check Point solution
§ 164.312(b)	<p>§ 164.312(b) <i>Audit controls</i></p> <p>Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.</p>	<p>As part of its core functionality, Check Point solutions monitor and log user activity, including access to EPHI. They record critical information like user, services and resources used, time, and date. SmartCenter provides a central console to view these events. Eventia Reporter provides a solution to report on events for auditing purposes. Eventia Analyzer provides a solution to identify an activity to be examined by an administrator that may involve EPHI.</p>
§ 164.312(c)(1)	<p>§ 164.312(c)(1) <i>Integrity (addressable)</i></p> <p>Implement procedures to protect EPHI from improper alteration or destruction.</p>	<p>IPS-1 is a dedicated intrusion prevention system that delivers mission-critical protection and granular forensic analysis capabilities and flexible deployment. IPS-1 helps protect against enterprise events such as database hacking, Web-site hacking and defacement, and the hacking of email servers that may contain EPHI.</p>
§ 164.312(d)	<p>§ 164.312(d) <i>Person or entity authentication (required)</i></p> <p>Implement procedures to verify the identity of a person or entity seeking access to EPHI.</p>	<p>Check Point access solutions, VPN-1 and Connectra, support password, token, digital certificate, and one-time password authentication for entities seeking access to protected EPHI, through both internal and external (OPSEC partnership) capabilities. Check Point provides integrated certificate authority (X.509 digital certification) for both user and entity authentication. This enables users to have strong authentication between different entities without having to deploy a separate certificate authority, thus providing a simpler means to comply. Check Point also supports shared secrets for VPNs and internally supports a user database with user names/ passwords or domain passwords.</p>

Technical Safeguards HIPAA Security Rule 164.312		
HIPAA Standard	Implementation specification (summary)	Check Point solution
<p>§ 164.312(e)(2)(i)</p> <p>§ 164.312(e)(2)(ii)</p>	<p>§ 164.312(e)(2)(i) <i>Transmission security integrity controls (addressable)</i></p> <p>Implement security measures to ensure that electronically transmitted EPHI is not improperly modified. Recommends the use of network communications protocols.</p> <p>§ 164.312(e)(2)(ii) <i>Encryption (addressable)</i></p> <p>Encrypt EPHI when transmitted over a communications network.</p>	<p>Check Point remote access solutions, VPN-1 and Connectra, provide strong encryption for data during transmission over open networks using standards-based encryption protocols. VPN-1 supports SSL- and IPSec-encrypted communication protocols. Connectra supports SSL- and TLS-encrypted communication protocols. In addition, both support the MD5 and SHA-1 protocols to ensure the integrity of secure transmissions involving cardholder data.</p> <p>VPN-1 UTM Edge W, which provides Wi-Fi access as part of the solution, employs IPSec-over-WLAN encryption and enables the regular rotation of WEP keys. It supplements WEP, WPA, and WPA with inspection by Check Point firewall, intrusion prevention, and antivirus technologies. Users who use IPSec-over-WLAN rather than WEP can be granted higher access rights, as well.</p> <p>Check Point VARs, SIs, and business partners can provide consulting services to deploy Check Point solutions within an organization to enable the secure exchange of data.</p>

For more detail on how individual Check Point products address HIPAA requirements, please contact your local Check Point representative.

Conclusion

Healthcare organizations that are not fully compliant with HIPAA are working to become so as soon as possible. Many organizations that are compliant seek to strengthen their systems and solutions to enable ongoing compliance. Building a solid foundation for security is not just a matter of reducing the risk of noncompliance, it is about good business practices—protecting and enhancing operational efficiencies, delivery of care, and the trust of patients and business partners. Through an integrated array of solutions that address key HIPAA requirements, Check Point provides a comprehensive means for building your security base. Healthcare organizations can use Check Point solutions to achieve a clean bill of health—in compliance and in business.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecureRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.