



# Endpoint Security Considerations for Achieving HIPAA Compliance

# Contents

Transformation of American Health Care Will Put Spotlight on Security .....	3
Overview of HIPAA Security .....	3
Planning for HIPAA Endpoint Compliance .....	3
Technologies for Endpoint Security .....	4
Best Practices for Deploying Endpoint Security Technologies .....	4
Endpoint Security Controls for HIPAA Compliance .....	5
Learn More .....	6

## Transformation of American Health Care Will Put Spotlight on Security

The new number-one priority for America is to improve the efficiency of the nation's healthcare system—especially in the information technology arena. Experts say rising health costs are the main cause of long-term national budget problems, and that computerization of health records will drive down costs. Computerization will also bring an operational sea change, for currently less than one out of every five doctors in the U.S. uses electronic health records. This change will accelerate requirements to ensure the confidentiality, integrity, and availability of electronic protected health information (EPHI). Securing these records is one element of HIPAA, the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191). In gauging threats to security of EPHI, unprotected endpoints constitute the largest source of potential breaches to personal health information.

## Overview of HIPAA Security

HIPAA covers five major aspects of health care. In 2003, the U.S. Dept. of Health and Human Services published the HIPAA Security Rule to safeguard EPHI. These security provisions are mandatory and apply to all healthcare providers (hospitals and physicians), healthcare payers (insurance companies and self-insured employers), and healthcare information clearinghouses. The federal government enforces these rules and organizations that do not comply will face potential administrative actions, fines, or criminal prosecution.

The HIPAA Security Rule requires the healthcare industry to use measures that keep personal health information secure and decrease the means of tampering, destruction, or inappropriate access to EPHI. The Security Rule specifies three types of controls to be used by organizations for compliance with HIPAA:

1. Administrative Safeguards - to document formal policies and practices for data protection, including the organization's security management process, and implementation specifications
2. Physical Safeguards - to protect data from the hazards of fire, weather, environment, or intrusion
3. Technical Safeguards - to protect data and control access to information by individuals, and guard against unauthorized access via a network

## Planning for HIPAA Endpoint Compliance

Endpoints are the universal Achilles heel of risk for HIPAA security compliance. Attacks increasingly bypass traditional perimeter-focused security and enter endpoints and the health organization network by many vectors. Mobile endpoints may be used outside the traditional perimeter of security controls. And it's difficult to manually ensure that all controls required for compliance are always operating effectively on every endpoint. Automation is vital. Choosing and using the right endpoint security technical controls is a key part of the HIPAA compliance process.

“The Check Point solution provides the secure foundation we need for compliance with the HIPAA rules for transmitting confidential patient information.”

Dr. John Daily  
Executive Director  
Encompass Medical Group

## Technologies for Endpoint Security

Deployment of standard endpoint security technologies will provide a robust and comprehensive multi-layer defense against exploits. These are essential security controls for verifying compliance—for HIPAA and other regulations.

Essential endpoint security technologies
<b>Firewall</b> —Blocks or allows traffic based on criteria defined by endpoint security policies.
<b>Intrusion Detection / Prevention System</b> —IDS/IPS technology analyzes network traffic for malicious code and attacks.
<b>Program Control</b> —Restricts network access on a per-program basis thereby limiting exposure to vulnerabilities and attacks.
<b>Network Access Control</b> —NAC restricts access by unknown users by enforcing policy compliance at endpoints and offering auto-remediation.
<b>Antivirus / Anti-spyware</b> —Scans files to identify infections and spyware based on a variety of technologies, and automatically executes responses.
<b>Data Security</b> —Automatic authentication of an endpoint user, encryption of data, and control of endpoint ports and removable media.
<b>Secure Remote Access</b> —Allows remote endpoints to safely access healthcare information via virtual private networks (VPNs).

## Best Practices for Deploying Endpoint Security Technologies

Prior to deployment of endpoint security technologies, several strategies must be considered to ensure flexibility, reliability and long term viability of the overall solution. Best practices should include:

**Deploy integrated solutions**—Choose solutions from reputable vendors that address multiple requirements. Integrated solutions can optimize management and administration efficiencies. This may not be possible with individual point solutions.

**Be holistic**—Deploy solutions that address core security capabilities and facilitate compliance with multiple regulations and industry guidelines.

**Add value**—Use solutions that enhance fundamental business value and differentiate your business, such as adding new sales channels.

**Ensure future scalability**—Deploy solutions that will adapt to and grow with changing business requirements.

## Endpoint Security Controls for HIPAA Compliance

HIPAA Endpoint Requirement*	Endpoint Security Control
.308(a)(1)(ii)(B) <b>Risk management</b> requires security measures to reduce risks and vulnerabilities affecting electronic protected health information (EPHI) to a reasonable and appropriate level	Best practices specify use of <b>all standard endpoint protection controls</b> including firewall, IDS/IPS, program control, network access control, antivirus and anti-spyware, data security, and remote access control.
.308(a)(1)(ii)(D) <b>Information system activity review</b> of logs and activity reports	Security software on each endpoint must <b>automatically post security events to audit log files.</b>
.308(a)(3)(ii)(A) and (4)(ii)(B-C) <b>Access authorization and/or supervision</b>	<b>Endpoint access control</b> technology automatically regulates network access. <b>Endpoint program control</b> technology provides granular application access control. <b>Endpoint firewall</b> restricts or allows network activity.
.308(a)(4)(ii)(A) Implement procedures that protect EPHI of a healthcare clearinghouse from <b>unauthorized access</b> by a larger parent organization	<b>Endpoint access control</b> automatically regulates network access. <b>Endpoint program control</b> technology provides granular application access control.
.308(a)(4)(ii)(A) Implement <b>periodic security updates</b>	<b>Endpoint policy compliance</b> is enforced by network access control technology, such as checking endpoints for the latest version of antivirus software, and auto-remediating endpoints into compliance before allowing access to EPHI.
.308(a)(5)(ii)(B) Implement procedures for <b>guarding against, detecting, and reporting malicious software</b>	<b>Antivirus.</b> Endpoints must run antivirus technology to automatically eliminate viruses and other malware. Defenses include signatures, behavior blockers, and heuristic analysis.
.308(a)(6)(ii) Implement policy and procedures to <b>identify and respond to suspected or known security incidents</b> , mitigate harm and document incidents	<b>Intrusion detection or prevention</b> technologies must include each endpoint that can access the cardholder data environment. Endpoint IDS/IPS must be integrated with the organization's standard security alert system.
.308(a)(7)(ii)(B) Implement procedures to <b>restore any loss of data</b>	<b>Endpoint data protection</b> technology should automatically create a centrally-stored recovery file for disaster recovery.
.308(a)(7)(ii)(C) Implement procedures for <b>obtaining necessary EPHI during an emergency</b>	<b>Endpoint access control</b> technology must automatically regulate remote network access based on centrally controlled policy, including provision of emergency passwords.
.308(b)(1) Any <b>business associate must provide assurance that it will safeguard all EPHI data</b> it has or transmits	Reports from <b>endpoint policy compliance</b> technology must document that each endpoint is operating all mandated security controls and the most current respective versions of security software.
.312(a)(2)(iv) and .312(a)(2)(ii) Implement a mechanism to <b>encrypt and decrypt EPHI</b>	<b>Endpoint encryption</b> solutions provide automatic full disk encryption, media encryption, and encryption for mobile devices such as personal digital assistants and smart phones.

\* Administrative and Technical Safeguards in HIPAA Final Security Rule 164.308-312

## Learn More

For more information about HIPAA requirements, please visit the U.S. Department of Health and Human Services Web site at:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>

For more information about how Check Point Endpoint Security solutions can help you comply with HIPAA requirements, please contact your local Check Point sales representative, call Check Point at 800-429-4391, or visit [www.checkpoint.com](http://www.checkpoint.com).



## About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is the leader in securing the Internet. Check Point offers total security solutions featuring a unified gateway, single endpoint agent and single management architecture, customized to fit customers' dynamic business needs. We are unique in this offering as a result of our leadership and innovation in the enterprise firewall, personal firewall/endpoint, data security and VPN markets.

Check Point's pure focus is on information security. Through its NGX platform, Check Point delivers a unified security architecture to protect business communications and resources, including corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market-leading endpoint and data security solutions with Check Point Endpoint Security products, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm solutions protect millions of consumer PCs from hackers, spyware and identity theft. 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: 972-3-624-1100  
email: [info@checkpoint.com](mailto: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>

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, 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, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, 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, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, 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 SecuRemote, 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.