New Boundary Technologies®
HIPAA Security Guide

A New Boundary Technologies
HIPAA Security Configuration Guide
Based on NIST Special Publication 800-68

1.0 Executive Summary

This HIPAA Security Guide was developed by New Boundary Technologies to provide insight and recommended security configurations for HIPAA Security Officers and Network Administrators charged with securing their networks to meet the HIPAA Final Security Rule. This guide is based on the High Security Level (which recently has been renamed as Specialized Security-Limited Functionality) recommendations from the National Institute of Standards and Technology (NIST) Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.* The complete version of 800-68 is available from NIST at: http://csrc.nist.gov/

When an IT security configuration template (e.g., hardening or lockdown guide) is applied to a system, in combination with trained system administrators and a sound and effective security program, a substantial reduction in vulnerability exposure can be achieved. In fact, actual testing by the NSA and NIST of these templates on workstations and servers has shown that they will reduce the vulnerabilities on systems from 80% to 90%. From a HIPAA security perspective, the correct application of a security template directly addresses a critical requirement under Administrative Safeguards; Standard: Security Awareness and Training - Protection from Malicious Software.

The above requirement is perhaps the most far-reaching yet least understood within the HIPAA Security Rule. The question most asked is just how does one meet this very broad requirement? The first thought is that one only needs to have the standard anti-virus, patch and spyware tools, along with the IT processes in place to use them, and that will meet the requirement. While these tools are critical to have in your network security tool kit, they are really tools that only address the *symptoms* of malicious software. They will tell you that a system has been infected and remove the infection, but they will not prevent an infection or tell you *how* the system got infected! They essentially only treat 10% to 20% of the vulnerabilities on your systems, but they don't treat the *cause* of the infection, which is a misconfigured system.

This is where the proper application of tested security policies provides a significant increase in security. Viruses and spyware exploit the software defects in applications and misconfigurations of the operating system. While you need good anti-virus, patch and spyware tools to detect and remove malware, those tools are not designed to correct problems in configuration areas such as insecure accounts, unnecessary services, file permissions, registry groups or values.

In the past, applying any security policy was a complex and time-consuming task that required use of numerous complex and separate tools for workstations and servers. Furthermore, once a system was "locked down" with a template or security baseline configuration, it was extremely hard to 1) Detect when a system became "unlocked" or non-compliant and 2) When non-compliance was discovered, it was a manual process to remediate the system and bring it back into compliance. For these reasons and others network administrators tended to avoid applying security templates to their systems and thus missed an opportunity to eliminate up to 90% of their system vulnerabilities.

To address the complexity of customizing, deploying, managing and maintaining security configurations and policies on desktops and servers, New Boundary Technologies developed Policy Commander™. Policy Commander is a ***single solution*** that contains scores of security policies that can be applied to both workstations and servers. It is no longer necessary to learn how to use separate tools and scripting languages for different versions of Windows workstations and servers. To further simplify the process of testing and applying the NIST Security Template, Policy Commander has reduced the numerous individual security settings contained in the NIST template to a smaller, more manageable collection of security policies. Thus from a central web console and database, Policy Commander can quickly deploy a complete Microsoft, NSA or NIST template or a single policy to one or all of your systems. Policy Commander then will continuously monitor the state of computers and security policies, notify users of any instances of non-compliance, and automatically remediate those non-compliant computers and security policies. Policy Commander is a solution that significantly reduces the complexity, time and effort to package, test, deploy, monitor and enforce any security policy on any Windows-based server or workstation located anywhere in you network worldwide.

To see how Policy Commander helps you meet the HIPAA Security Rule, see Appendix A which provides a HIPAA Security Rule/Policy Commander Crosswalk.

To download a full Policy Commander Evaluation version please visit the New Boundary website: http://www.newboundary.com/products/policycommander/index.htm

2.0 NBT HIPAA Security Guide

The purpose of this guide is to show how Policy Commander can secure local Windows XP workstations and Windows servers within a HIPAA environment. The NIST Specialized Security-Limited Functionality template modifies several key areas of a Windows XP system, including password policy, account lockout policy, auditing policy, user rights assignment, system security options, event log policy, system service settings, and file permissions. The template is based on security templates previously developed by the National Security Agency (NSA), Defense Information Systems Agency (DISA), and Microsoft. Most of the settings in the template represent consensus recommendations as proposed by various security experts from the Center for Internet Security (CIS), DISA, NSA, Microsoft, and NIST.

While NIST has developed different template settings for use in Small Office/Home Office (SOHO), Legacy, Enterprise and High Security environments, NIST has recommended that any company that has to comply with the HIPAA Security Rule should look at using the XP Specialized Security-Limited Functionality template discussed in this guide. Therefore, New Boundary Technologies recommends that any systems that will handle Electronic Protected Health Information (EPHI) use or be migrated to the Windows XP operating system. This will not only provide the highest level of security but significantly ease the task of testing, applying and maintaining the Specialized Security-Limited Functionality template for Windows XP.

2.1 High Security Environment

A high security environment is any environment, networked or standalone, which is at high risk of attack or data exposure. This environment encompasses computers that contain highly confidential information (e.g., personnel records, medical records, financial information) and perform vital organizational functions (e.g., accounting, payroll processing, air traffic control). These computers might be targeted by external parties for exploitation, but also might be targeted by trusted parties inside the organization. A high security environment could be a subset of a SOHO or Enterprise environment. For example, three desktops in an enterprise environment that hold confidential EPHI could be thought of as a high security environment within an enterprise environment. In addition, a laptop used by a mobile healthcare worker might be a high security environment within a SOHO environment. A high security environment might also be a self-contained environment outside any other environment: for instance, a government security installation dealing in sensitive data.

Systems in high security environments face threats from both insiders and external parties. Because of the risks and possible consequences of a compromise in a high security environment, it usually is the most restrictive and secure configuration. The suggested configuration provides the greatest protection at the expense of ease of use, functionality, and remote system management. In a high security environment, this guide is targeted at experienced security specialists and seasoned system administrators who understand the impact of implementing these strict requirements.

2.2 Best Practices for Analysis and Testing of Security Policies

Although the NIST security settings have undergone considerable testing and are recommended for companies dealing with HIPAA security, every system and environment is unique, so system administrators should perform their own testing. The development of the NIST Windows XP Specialized Security-Limited Functionality Template was driven by the need to create a more secure Windows XP workstation configuration. Because some settings in the templates may reduce the functionality or usability of the system, it is not recommended that the complete template be used as a baseline security configuration. Specific settings in the templates should be modified as needed so that the settings conform to local policies and support required system functionality. New Boundary strongly recommends that organizations fully test the HIPAA policies contained in Policy Commander on representative systems before widespread deployment. Some settings may inadvertently interfere with applications, particularly legacy applications that may require a less restrictive security profile.

NBT recommends the following steps be taken to test the policies:

1) **Analyze:** Conduct a risk assessment of the assets in your network that will handle EPHI. Use Policy Commander as part of the risk assessment to compare the current security policies of the local workstation/servers to the policies required to meet the HIPAA Security Rule.

2) Test: When new security settings or policies are applied, they can interfere with the operation of existing software applications and other operations on the target computers. We strongly recommend testing each new policy thoroughly in the test environment before moving it to the production environment. Our recommended testing methodology includes the following steps:

- System administrators build their systems from a clean formatted state to begin the process of securing Windows XP workstations.
- System administrators should perform the installation and test process on a secure network segment or off the organization's network until the security configuration is completed.
- All patches, service packs, hotfixes and rollups for XP should be applied.
- All desktop or server applications should be installed, operational and have all upgrades/patches applied.
- Strong passwords should be set for all accounts.

3) **Assign:** Use Policy Commander to install the NIST policy modules in the test mode.

In the past, network administrators would have to apply the entire template and then spend hours troubleshooting the dozens of settings to see which ones caused a problem on the test workstation. By reducing the number of settings to a small collection of key policies, network administrators now can individually apply each policy, modify it as necessary, and then add the next policy. This will significantly decrease the time required to test and configure the HIPAA security configuration that best fits your environment.

The NBT HIPAA security policies are organized based on the nine categories identified by NIST. Those categories are:
1) Account Policies
2) Local Policies
3) Event Log Policies
4) Restricted Groups
5) System Services
6) File Permissions
7) Registry Permissions
8) Registry Values
9) File and Registry Auditing

Appendix B provides an overview of these nine categories and which New Boundary Technologies HIPPA Security Policies are in each category.

4) **Enforce:** Save final security configuration baseline, use Policy Commander to organize your key HIPAA workstations and servers, and then deploy the HIPAA security configuration baseline. New Boundary recommends that the automatic enforcement feature be utilized to ensure complete 24x7 enforcement of the HIPAA security configuration.

For a complete overview of how Policy Commander works download the 30 day trial version at: ***http://www.newboundary.com/products/policycommander/index.htm.***

3.0 Summary of Recommendations

- Protect each system based on the potential impact to the system of a loss of confidentiality, integrity, or availability.
- Reduce the opportunities that attackers have to breach a system by limiting functionality according to the principle of least privilege and resolving security weaknesses.
- Select security controls that provide a reasonably secure solution while supporting the functionality and usability that users require.
- Use multiple layers of security so that if one layer fails or otherwise cannot counteract a certain threat, other layers might prevent the threat from successfully breaching the system.
- Conduct risk assessments to identify threats against systems and determine the effectiveness of existing security controls in counteracting the threats. Perform risk mitigation to decide what additional measures (if any) should be implemented.
- Document procedures for implementing and maintaining security controls. Maintain other security-related policies and documentation that affect the configuration, maintenance, and usage of systems and applications, such as acceptable use policy, configuration management policy, and IT contingency plans.
- Test all security controls, including the settings in the NIST security templates, to determine what impact they have on system security, functionality, and usability. Take appropriate steps to address any significant issues.
- Monitor and maintain systems on a regular basis so that security issues can be identified and mitigated promptly. Actions include acquiring and installing software updates, monitoring event logs, providing remote system administration and assistance, monitoring changes to OS and software settings, protecting and sanitizing media, responding promptly to suspected incidents, performing vulnerability assessments, disabling and deleting unused user accounts, and maintaining hardware.

Appendix A

HIPAA Security Rule/Policy Commander Crosswalk

This guide provides a matrix that correlates the Administrative, Technical and Physical Standards and Implementation Specifications of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule to applicable features/functionality of New Boundary Technologies' Policy Commander solution. Organizations can use Policy Commander to implement security policies that support the HIPAA Security Rule on Windows workstations and servers.

NOTE: Items in **bold text** represent the 18 HIPAA Standards, which typically have a subset of requirements for compliance.

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Policy Commander Capabilities
Administrative Safeguards		
164.308(a)(1)(i)	**Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.**	
164.308(a)(1)(ii)(A)	Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Use Policy Commander to assess current security policy configuration and risk.
164.308(a)(1)(ii)(B)	Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a)	Use Policy Commander to apply the HIPAA Policy Library based on the NIST Security Templates in NIST Special Publication 800-68.
164.308(a)(1)(ii)(C)	Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	N/A
164.308(a)(1)(ii)(D)	Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Policy Commander continuously reviews and maintains audit logs, access reports, and security incident tracking reports.

164.308(a)(2)	**Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.**	Use Policy Commander to develop, implement and monitor workstation and server security policies.
164.308(a)(3)(i)	**Workforce Security: 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.**	
164.308(a)(3)(ii)(A)	Authorization and/or Supervision (A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Policy Commander can restrict access to workstations and servers to only authorized workforce members.
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure (A): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	N/A
164.308(a)(3)(ii)(C)	Termination Procedure (A): Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	N/A
164.308(a)(4)(i)	**Information Access Management: 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.**	
164.308(a)(4)(ii)(A)	Isolating Health Clearinghouse Functions (R): If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from	A Clearinghouse can use Policy Commander to implement the same security policies as the larger organization.

	unauthorized access by the larger organization.	
64.308(a)(4)(ii)(B)	Access Authorization (A): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	The Policy Commander HIPAA Policy Library contains recommended security policies that secure access to electronic protected health information. Policy Commander can also be used as a Secure Access Gateway for mobile or remote users. Use the Policy Editor to create access policies that will be checked and remediated on all user systems before they are allowed access to the internal network. This can also be applied to all Business Associates who have access to the internal network.
164.308(a)(4)(ii)(C)	Access Establishment and Modification (A): Implement policies and procedures that, based upon the entity's access authorization policies, establish document, review and modify a user's right of access to a workstation, transaction, program, or process.	The Policy Commander HIPAA Policy Library contains recommended security policies that will establish access control to workstations that contain electronic protected health information.
164.308(a)(5)(i)	**Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).**	
164.308(a)(5)(ii)(A)	Security Reminders (A): Periodic security updates.	Policy Commander will automatically provide security updates to workstations and servers.
164.308(a)(5)(ii)(B)	Protection from Malicious Software (A): Procedures for guarding against, detecting and reporting malicious software.	Applying the HIPAA Policy Library will reduce system vulnerabilities by over 90% and is key to complying with the HIPAA Security Rule.
164.308(a)(5)(ii)(C)	Log-in Monitoring (A): Procedures for monitoring log-in attempts and reporting discrepancies.	N/A
164.308(a)(5)(ii)(D)	Password Management (A): Procedures for creating, changing, and safeguarding passwords.	N/A
164.308(a)(6)(i)	**Security Incident Procedures: Implement policies and procedures**	

	to address security incidents.	
164.308(a)(6)(ii)	Response and Reporting (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Policy Commander will automatically identify, respond and correct suspected and known security policy incidents. Policy Commander will document/log security incidents and provide full reports for audits.
164.308(a)(7)(i)	**Contingency Plan: 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.**	
164.308(a)(7)(ii)(A)	Data Backup Plan (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	N/A
164.308(a)(7)(ii)(B)	Disaster Recovery Plan (R): Establish (and implement as needed) procedures to restore any loss of data.	N/A
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan (R): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	N/A
164.308(a)(7)(ii)(D)	Testing and Revision Procedure (A): Implement procedures for periodic testing and revision of contingency plans.	N/A
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components.	N/A
164.308(a)(8)	**Evaluation: 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**	Policy Commander continuously provides real-time evaluation, enforcement and reporting of the HIPAA security configuration selected.

	information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	
164.308(b)(1)	**Business Associate Contracts and Other Arrangements: A covered entity, in accordance with §164.306, 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 Section 164.314(a) that the business associate will appropriately safeguard the information.**	A business associate can use Policy Commander to implement the same security policies as the covered entity. Policy Commander can also be used by the covered entity as a Remote Access Gateway to enforce selected security policies and configurations on business associate's workstations requesting access to the network.
164.308(b)(4)	Written Contract or Other Arrangement (R): Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).	N/A

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Policy Commander Capabilities
Physical Safeguards		
164.310(a)(1)	**Facility Access Controls: 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.**	
164.310(a)(2)(i)	Contingency Operations (A): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	N/A
164.310(a)(2)(ii)	Facility Security Plan (A): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.	N/A
164.310(a)(2)(iii)	Access Control and Validation	N/A

	Procedures (A): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	
164.310(a)(2)(iv)	Maintenance Records (A): Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks.	N/A
164.310(b)	**Workstation Use: 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 that can access electronic protected health information.**	Use Policy Commander to create custom security policies that will restrict improper functions, such as unauthorized applications, changes to admin rights, access to files, etc from being executed on the workstation by end users.
164.310(c)	**Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.**	N/A
164.310(d)(1)	**Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of those items within the facility.**	
164.310(d)(2)(i)	Disposal (R): Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	N/A
164.310(d)(2)(ii)	Media Re-Use (R): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.	Policy Commander contains policies that will prevent the attachment and/or use of portable USB storage devices.
164.310(d)(2)(iii)	Accountability (A): Maintain a record of the movements of hardware and electronic media and any person responsible thereof.	N/A

164.310(d)(2)(iv)	Data Backup and Storage (A): Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	N/A

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Policy Commander Capabilities
Technical Safeguards		
164.312(a)(1)	**Access Control: 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 §164.308(a)(4).**	
164.312(a)(2)(i)	Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity.	N/A
164.312(a)(2)(ii)	Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	N/A
164.312(a)(2)(iii)	Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Policy Commander contains a policy that can be set to automatically log off a user after a set time limit.
164.312(a)(2)(iv)	Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information.	N/A
164.312(b)	**Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.**	
164.312(c)(1)	**Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.**	
164.312(c)(2)	Mechanism to Authenticate Electronic	Policy Commander contains a

	Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in any unauthorized manner.	policy that can restrict access to files or folders that contain electronic protected health information to only those with authorized access.
164.312(d)	**Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.**	Use the above File/Folder Access policy to help verify access to files or folders containing electronic protected health information.
164.312(e)(1)	**Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.**	N/A
164.312(e)(2)(i)	Integrity Controls (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	The policy that can restrict access to files or folders that contain electronic protected health information can also ensure that the information is not improperly modified without detection until disposed of.
164.312(e)(2)(ii)	Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	N/A

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Policy Commander Capabilities
Administrative and Organizational Requirements		
164.314(a)(1)	**Business Associate Contracts or Other Arrangements: (i) The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in §164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation**	

	under the contract or other agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful – (A) Terminate the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.	
164.314(a)(2)(i)	Business Associate Contracts (R): The contract between a covered entity and a business associate must provide that the business associate will – (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.	A business associate can use Policy Commander to implement the same security policies as the covered entity. Policy Commander can also be used by the covered entity as a Remote Access Gateway to enforce selected security policies and configurations on the business associate's workstations requesting access to the network.
164.314(a)(2)(ii)	Other Arrangements (R): When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if – (1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or (2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.	A business associate can use Policy Commander to implement the same security policies as the covered entity. Policy Commander can also be used by the covered entity as a Remote Access Gateway to enforce selected security policies and configurations on the business associate's workstations requesting access to the network.
164.314(b)(1)	**Requirements for Group Health Plans: Except when the only electronic protected health information disclosed to a plan**	

	sponsor is discloses pursuant to §164.504(f)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	
164.314(b)(2)(i)	Group Health Plan Implementation Specification (R): the plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to – (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.	A business associate can use Policy Commander to implement the same security policies as the covered entity. Policy Commander can also be used by the covered entity as a Remote Access Gateway to enforce selected security policies and configurations on the business associate's workstations requesting access to the network.
164.314(b)(2)(ii)	Group Health Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsors to – (ii) Ensure the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.	A business associate can use Policy Commander to implement the same security policies as the covered entity. Policy Commander can also be used by the covered entity as a Remote Access Gateway to enforce selected security policies and configurations on the business associate's workstations requesting access to the network.
164.314(b)(2)(iii)	Group Health Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to – (iii) Ensure that any agent, including a subcontractor, to whom it provides the information agrees to implement reasonable and appropriate security measures to protect the information.	N/A
164.314(b)(2)(iv)	Group Health Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to – (iv) Report to the group health plan any security incident of which it becomes aware.	N/A

164.316(a)	**Policies and Procedures: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.**	Policy Commander complements other HIPAA solutions designed to create the covered entity's HIPAA Security Policy Manual. Policy Commander deploys, monitors, and automatically remediates those specific HIPAA security policies that apply to workstation and server security.
164.316(b)(1)	**Documentation: (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.**	Policy Commander continuously maintains electronically the security policies and procedures implemented to meet the HIPAA Security Rule. Policy Commander also maintains a printable record of any action, activity, or assessment conducted on the security configuration established by the covered entity. This record can be provided to any HIPAA auditor.
164.316(b)(2)(i)	Time Limit (R): Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	N/A
164.316(b)(2)(ii)	Availability (R): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Available with Policy Commander.
164.316(b)(2)(iii)	Updates (R): Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	Available with Policy Commander.

Appendix B

New Boundary Technologies HIPAA Template Settings

This chart describes the security policies contained in the New Boundary Technologies HIPAA Windows XP High Security Template. These policies are organized into nine key security categories based on the National Institute of Standards and Technology (NIST) publication SP800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule.* The New Boundary Technologies template contains the recommended settings from the NIST XP High Security Template but also contains custom policies developed by New Boundary Technologies to meet specific HIPAA security requirements. Applying these security policies meets the critical HIPAA Administrative Safeguard 164.308(a)(5)(i), Security Awareness and Training: 164.308(a)(5)(ii)(B) Protection from Malicious Software.

Security Categories	Policy Commander Policies
1.0 Account Policies	• Harden account lockout settings
2.0 Local Policies 2.1 Audit Policies 2.2 User Rights Assignment 2.3 Security Options	• Control the System Audit Policy settings • Harden the User Rights Assignment settings • Disable the Guest Account • Limit local account use of blank passwords to console only • Harden Device settings • Harden Domain Member settings • Harden Interactive Logon settings • Harden Microsoft network server settings • Harden network access settings • Harden network security settings • Harden Recovery Console settings • Harden Shutdown settings • Enforce FIPS Certified Cryptography • Harden System Objects settings • Shut down immediately if unable to log security audits • Disallow anonymous SID_Name translation • Force logoff when logon hours expire
3.0 Event Log Policies	• Control Event Log settings
4.0 Restricted Groups	• Remove all users from the Remote Desktop Users and Power Users groups.
5.0 System Services	• Alerter • Clip book • FTP Publishing • HS Admin Service • Messenger • NetMeeting Remote Desktop Sharing • Routing and Remote Access • Simple Mail Transfer Protocol (SMTP)

	• Simple Network Management Protocol (SNMP) Service • SNMP Trap • Telnet • World Wide Web Publishing Services • Computer Browser • Remote Registry • Task Scheduler • Terminal Services • Fax Service • Indexing Service • Remote Desktop Help Session Manager • Universal Plug & Play Device Host • Net logon
6.0 File Permissions	• Harden security permissions for critical files
7.0 Registry Permissions	• Harden security permissions for critical registry keys
8.0 Registry Values 8.1 Debugging 8.2 Automatic Functions 8.3 Networking	• Disable the Dr. Watson debugger and memory dump file • Disable automatically running CD-ROMs • Disable automatic administrator logon • Disable automatic reboot • Strengthen miscellaneous networking settings • Harden the Microsoft TCP/IP stack settings
9.0 Custom HIPAA Policies 9.1 Automatic Logoff 9.2 EPHI File Protection 9.3 USB Removable Device	• Meets HIPAA Administrative Safeguard 164.308(a)(4)(ii)(B) & (C): Access Authorization and Access Establishment • Meets HIPAA Technical Safeguard 164.312(c)(1) & (2); Integrity and Mechanism to Authenticate Electronic Protected Health Information • Meets HIPAA Physical Safeguards 164.310(d)(2)(ii) Media Re-Use

# # #