PatchLink Security Configuration Management™

HIPAA, the Health Insurance Portability and Accountability Act, sets a high standard for information security. The 2003 regulations (CFR 164.306) state that organizations handling medical data must:

> (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
> (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

Today, cybercrime exceeds illegal drugs as the world's number one crime and "any reasonably anticipated threat" covers a wide range of hazards. Information systems are under attack on a daily basis, and even small mistakes can be costly. One misconfigured firewall can allow access to an entire network of customer information. For example, 45 million customer records from retailer TJX were compromised due to a single poorly secured wireless router.

A significant problem in HIPAA compliance is determining what constitutes a "reasonably anticipated threat". National Institute of Standards and Technology (NIST) guidance provides a cost effective answer. Under NIST 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPPA) Security Rule, organizations are required to:

1. **Characterize** their information systems
2. Select their **safeguards** (NIST 800-53)
3. **Assess their risks** (NIST 800-30) to determine what is a "reasonably anticipated threat"

Patchlink Security Configuration Management™ (SCM) makes HIPAA compliant risk assessments easy.

PatchLink technology provides support for all three of the basic HIPAA compliance tasks. PatchLink Scan™ provides continuously updated system **characterization**. Patchlink SCM™ provides a comparison of existing **safeguards** with NIST 800-53 requirements and uses the configuration and safeguard information to automatically **calculate risks** to protected information.

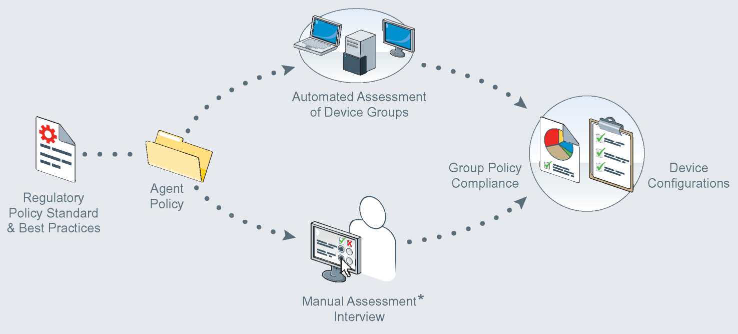
How It Works and What It Can Monitor

Policy Import
Import of policy standards according to SCAP checklists (e.g. FDCC).

Automated Assessment
Used with PatchLink Update™ or PatchLink Scan™, automated assessment against the checklist is performed.

Manual Assessment*
In order to be exhaustive, manual assessment Interview allows the mapping of non-IT automated security checks such as physical security checks.

Policy Compliance Management & Reporting
Both automated assessment and manual assessment interview checks are consolidated to provide a comprehensive compliance monitoring and reporting tools

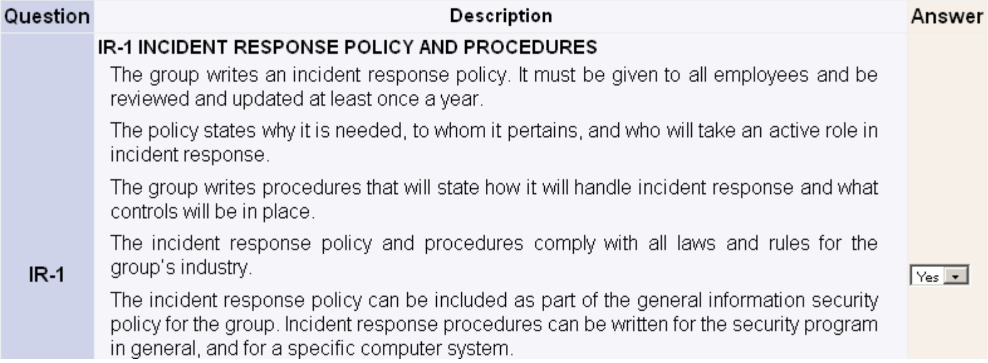


Automated Assessment of Device Groups
Regulatory Policy Standard & Best Practices
Agent Policy
Group Policy Compliance
Device Configurations
Manual Assessment* Interview

- Event Log Policy Settings
- File Permission Settings
- Local policies Group
- System Services Group
- Network Settings
- System Settings
- Windows Components
- Local User Policy Settings
- Security Patches
- Firewall Settings
- IE Settings
- Application Settings

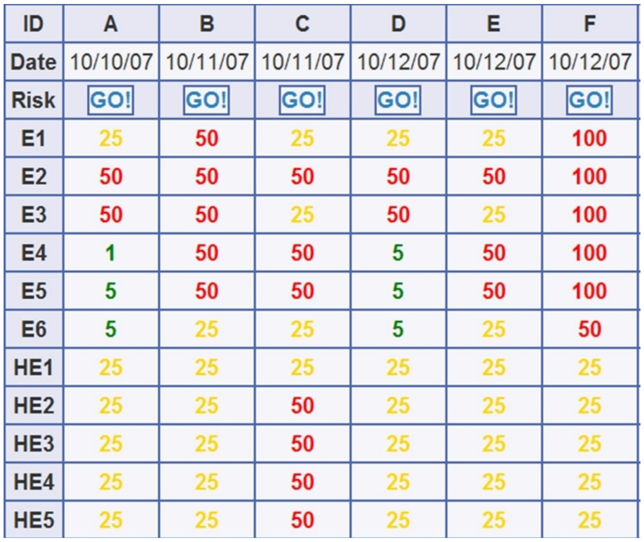
The easily interpreted reports can rapidly communicate changes in risks to protected information. The automated risk assessment reports can be updated as often as daily, with alarms sent by text message or email when risks increase beyond pre-set limits.

PatchLink SCM™ utilizes SCAP checklist and Policy Questionnaire data (shown below) to generate risk assessments. The output of the combined automated/manual PatchLink assessment process provides a continuously updated picture of network compliance with standards provided by the NIST.



Question	Description	Answer
IR-1	**IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES** The group writes an incident response policy. It must be given to all employees and be reviewed and updated at least once a year. The policy states why it is needed, to whom it pertains, and who will take an active role in incident response. The group writes procedures that will state how it will handle incident response and what controls will be in place. The incident response policy and procedures comply with all laws and rules for the group's industry. The incident response policy can be included as part of the general information security policy for the group. Incident response procedures can be written for the security program in general, and for a specific computer system.	Yes

A significant challenge for medical information managers is dealing with business associates that need access to protected information. Under the security rule, information owners are liable for business associate misuse of information "unless the covered entity took reasonable steps to cure the breach". Reporting using the PatchLink SCM technology can provide continuously updated risk assessments for each business associate.



ID	A	B	C	D	E	F
Date	10/10/07	10/11/07	10/11/07	10/12/07	10/12/07	10/12/07
Risk	GO!	GO!	GO!	GO!	GO!	GO!
E1	25	50	25	25	25	100
E2	50	50	50	50	50	100
E3	50	50	25	50	25	100
E4	1	50	50	5	50	100
E5	5	50	50	5	50	100
E6	5	25	25	5	25	50
HE1	25	25	25	25	25	25
HE2	25	25	50	25	25	25
HE3	25	25	50	25	25	25
HE4	25	25	50	25	25	25
HE5	25	25	50	25	25	25

This group risk monitoring can allow summary review of information security for several hundred networks from a single console. The "Enterprise" risk management system is ideal for hospitals and clinics with dozens or hundreds of business associates.

Site #	PKI	Site #	PKI	Site #	PKI	Site #
1	25:606	32	25:750	63	10:275	94
2	25:750	33	10:275	64	100:2550	95
3	25:550	34	100:2550	65	10:300	96
4	25:425	35	10:300	66	10:250	97
5	25:650	36	10:250	67	100:390	98
6	10:300	37	10:300	68	100:2550	99
7	50:775	38	10:250	69	10:300	100
8	50:340	39	100:390	70	10:250	101
9	50:450	40	10:275	71	100:2550	102
10	50:550	41	100:2550	72	10:300	103
11	50:400	42	10:300	73	10:250	104
12	25:425	43	10:250	74	100:390	105
13	10:155	44	100:390	75	100:2550	106

HIPAA compliance with the Security Rule is a constant challenge due to attacks from a wide variety of increasingly sophisticated sources. Patchlink Security Configuration Management™ tools can make meeting the challenge more possible and less expensive. In tough times, better security at lower cost is imperative.

For more information on Security Configuration Management™ or other PatchLink products, your Lumension representative or go to www.lumension.com.