Guide:
Meeting HIPAA Security Rules
Introduction
Securing patient information and confidentiality is no easy task. The CIO’s who are charged with the protection of healthcare information have found themselves surrounded by a new set of Federal rules and regulations governing the security and accessibility of electronic medical data transmissions internally and externally. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed by President Clinton on July 21, 1996 and designed to protect health insurance coverage of workers and their families as they would change jobs or lose them.

HIPAA Privacy Rule became effective April 14, 2003. As a result every healthcare organization including hospitals, doctors clinics, imaging and/or emergency care centers that sign-in patient records via a computer will be affected by the new set of business continuity and security rules that HIPAA imposes. Now, more than ever, there is an official need to more tightly control and audit access to patient information. These organizations are ordered to encrypt data communicated over open or public networks, to insure that patient data retained is accurate and accessible, and requirements for digital signatures are implemented and audited.

HIPAA Implications
HIPAA is the most sweeping legislation to affect the healthcare industry in over 30 years, both government and commercial players alike. Every HIPAA defined administrative transaction between healthcare providers and payers which are exchanged electronically will be subject to security standards contained within HIPAA regulations. In addition, all other organizations involved in such electronic exchange, such as those operating on behalf of providers and payers, intermediaries, and clearinghouses, will also be subject to the same standards. HIPAA will have varying degrees of implications in the market as each healthcare organization will have its own specific situations which will dictate the actions needed to be taken to become compliant. Overall, the total combined impact of HIPAA to healthcare organizations is at least on a par with that of the year 2000 impact and may be considerably larger in some cases.

Lockdown Networks  Provides Easy Compliance
Lockdown Networks enables fast and easy compliance with new security standards outlined in HIPAA Final Rule 45 CFR Part 164.308. Our automation of Vulnerability Assessment will dramatically lower operational costs of securing your network. Vulnerability Assessment is the systematic ‘proactive’ approach to security auditing. Security managers can rely on on-demand security audits that are available 24x7 and free of human error.

Read official text of “HIPAA: Final Rule for Security Standards”
Department of Health and Human Services, February 20, 2003
Who Must Comply with HIPAA?
The final rule for HIPAA regulations applies to any health plan, any healthcare clearinghouse, and any health care provider or payer that electronically maintain or transmit any healthcare information relating to an individual.

HIPAA regulations apply to all healthcare organizations for all transactions. Healthcare organizations conducting transactions through an agent or third party must also assure that the agent meets the same HIPAA rules and requirements that apply to them. HIPAA security standard is applicable to all healthcare information electronically maintained or used in an electronic transmission, regardless of format (standard transaction or proprietary format), including corporate entities.

HIPAA’s Three Security Standards
Safeguards must be met in the following three categories:

1. **Administrative Procedures**. Administrative policies and procedures governing confidentiality, integrity, and access of patient data.

2. **Physical Safeguards**. Business Continuity planning to safeguard patient data, control its access and protect the computer systems and networks that store and communicate that data from fire and other types of catastrophic disasters.

3. **Technical Safeguards**. Technical standards address access, authentication, authorization, auditing, integrity and the transmission of sensitive data.

**Administrative Procedures**
The healthcare organization being regulated must establish and document policies for providing their employees and other authorized users of systems differing levels of access to patient information based on a legitimate business need. There must also be established ongoing internal audit control mechanisms to record and to examine requests for patient information from information systems. These mechanisms would track logins, file access, and security related incidents. This is accomplished by performing internal and external evaluations of computer systems and network designs for proper security.

**Physical Safeguards**
Physical safeguards include physical access to the facility, workstation accessibility, workstation security, and device and media control. Confidential data on electronic media need to be tracked and encrypted. This includes transmissions using all media, even when the transmission is physically moved from one location to another using magnetic tape, disk, or CD media. Furthermore, wireless and other network access points must only allow authorized users access.
**Technical Safeguards**

Technical safeguards can be divided into two categories: security services and security mechanisms & Digital Signature.

**Technical Security Services.** Security measures to protect data stored within information systems. Transmission of any and all information containing patient identifiable information must be secure and private. Any transmissions over the Internet, Extranet, leased lines, dial-up lines, and private networks are to be secured and protected, although telephone voice response and faxback systems are not currently included.

**Technical Security Mechanisms & Digital Signature.** Security measures to prevent eaves-dropping and other types of inappropriate access to patient information communicated over networks. Data transmitted over electronic communications network needs to be secure and encrypted. An organization must also make sure all external parties (partners and other health organizations) are also in compliance with HIPAA.

**When are HIPAA Compliance Deadlines?**

Healthcare organizations are required to comply with HIPAA standards within two years or three years for small health plans. The chart below outlines compliance deadlines for HIPAA.

<table>
<thead>
<tr>
<th>Regulation (all final rules)</th>
<th>Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Transaction Rule Compliance w/o Extension</td>
<td>Oct. 2002</td>
</tr>
<tr>
<td>Privacy Rule Compliance</td>
<td>Apr. 2003</td>
</tr>
<tr>
<td>Electronic Transaction Rule Compliance</td>
<td>Oct. 2003</td>
</tr>
<tr>
<td>Privacy Rule Compliance for Small Health Plans</td>
<td>Apr. 2004</td>
</tr>
<tr>
<td>Security Rule Compliance</td>
<td>Apr. 2005</td>
</tr>
</tbody>
</table>

**Source:** U.S. Dept. of Health & Human Services

**Penalties for noncompliance**

HIPAA Privacy Rule is federal law, and any person or organization found not in compliance can face up to $250,000 in fines and up to 10 years in prison.

**Lockdown Networks Cost-Saving Solution**

In developing its vulnerability assessment solution, Lockdown Networks designed a system capable of meeting core administrative safeguard standards found in the Final Security Regulations. Our Lockdown™ products improves operational efficiency and is scalable to your organization’s needs. Security audit reports can be viewed anytime through an easy-to-use web-based interface. Bottom line, our products are guaranteed to reduce operation costs.
How Lockdown Networks can help you meet compliance rules

The Administrative Safeguard Standards (HIPAA Final Rule 45 CFR Sec. 164.308) were implemented to address security management process; assigned security responsibility; workforce security; information access management; security awareness and training; security incident procedures; contingency plan; evaluation; business associate contracts and other arrangements.

Compliance with the following specific requirements can be achieved at reduced cost with fewer resources utilizing vulnerability assessment products from Lockdown Networks:

<table>
<thead>
<tr>
<th>TITLE</th>
<th>SECTION</th>
<th>OBLIGATION</th>
<th>SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process (&quot;SMP&quot;)</td>
<td>164.308</td>
<td>Implement policies and procedures to prevent, detect, contain, and correct security violations.</td>
<td>Lockdown Appliance</td>
</tr>
<tr>
<td>SMP (Risk Analysis)</td>
<td>(a)(1)(i)</td>
<td>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.</td>
<td>Lockdown Appliance</td>
</tr>
<tr>
<td>SMP (Risk Management)</td>
<td>(a)(1)(ii)(A)</td>
<td>Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 163.306(a).</td>
<td>Lockdown Appliance</td>
</tr>
<tr>
<td>SMP (Information Systems Activity Review)</td>
<td>(a)(1)(ii)(D)</td>
<td>Implement procedures to regularly review records of information systems activity such as audit logs, access reports and security incident tracking reports.</td>
<td>Lockdown Appliance</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
<td>(a)(5)(i)</td>
<td>Implement a security awareness and training program for all members of its workforce (including management).</td>
<td>Lockdown Appliance</td>
</tr>
<tr>
<td>Security Incident Procedures (&quot;SIP&quot;)</td>
<td>(a)(6)(i)</td>
<td>Implement policies and procedures to address security incidents.</td>
<td>Lockdown Appliance</td>
</tr>
<tr>
<td>SIP (Response and Reporting)</td>
<td>(a)(6)(ii)</td>
<td>Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents and their outcomes.</td>
<td>Lockdown Appliance</td>
</tr>
<tr>
<td>Evaluation</td>
<td>(a)(8)</td>
<td>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 information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.</td>
<td>Lockdown Appliance</td>
</tr>
</tbody>
</table>

In addition, the Final Security Regulations require all covered entities to appoint a security official and assign the covered entity's security responsibilities to that individual. This security official would be responsible for monitoring and performing security audits on a continuous risk management cycle.
Try Lockdown Networks Vulnerability Management Products!
Lockdown Networks has created the most cost effective and efficient answer to network vulnerability management and remediation to date. It is proactive, current, scalable and flexible. For additional information, contact one of our authorized resellers or visit our website at www.lockdownnetworks.com

Lockdown Networks can arrange a “live” demonstration of our solution at your earliest convenience!

About Lockdown Networks, Inc.
Lockdown Networks, Inc. is the leader in next-generation, appliance-based security management for wired and wireless enterprise networks. Lockdown Networks’ Lockdown security products reduce business risk exposure and enable IT teams to increase their productivity by identifying where to spend budget for maximum benefit. Lockdown is the best practice approach to effective network security assurance. For more information, visit www.lockdownnetworks.com.

Contact Information:
Lockdown Networks
100 W Harrison, North Suite 300
Seattle, Washington 98119
206. 285. 8080
866. 844. 8080
www.lockdownnetworks.com