The HIPAA Security Rule & How to Prevent Vulnerabilities

Vulnerability Assessments provide healthcare administrators with the knowledge to understand and respond to security gaps and the latest threats. Audit information systems, assess remediation plans, and acknowledge ongoing security compliances using enterprise-grade vulnerability assessments deployed from a global cloud management console by utilizing infrastructure scans through the secure, convenient CES portal.

✉ info@usclaro.com
🌐 Vulnerability Assessment
☎ 833-992-5276

Claro
Enterprise Solutions

The Challenge

With 125 healthcare data breaches documented since April, the demand for 24/7 comprehensive cybersecurity has never been more pressing. And with the FBI requiring ALL attacks to be disclosed, plus the recent HIPAA Security Rule cracking down further and enforcing patient care facilities to:

1. Secure the confidentiality, integrity, and availability of electronically protected health information (EPHI) that it produces, receives, manages, or shares.

2. Defend against any reasonably anticipated threats to the security or integrity of EPHI.

3. Protect against uses or disclosures of information that are not permitted.

The urgency to ensure HIPAA/network security is at an all-time high. The problem? With thousands of lost, stolen, outdated, and unprotected devices processing and sharing sensitive HIPAA data and some attacks impacting over 50,000 users, cybercriminals are minimally deterred from accessing confidential patient information.

The Solution

To start, facilities should prioritize knowing the requirements of the six main sections of the HIPAA Security Rule…

1. **Security standards:**
The general requirements all facilities must follow. This first section establishes strategy flexibility, identifies standards and implementation specifications, outlines decisions a covered entity must make regarding addressable implementation specifications, and requires maintenance of security measures to continue reasonable and appropriate protection of EPHI.

2. **Administrative Safeguards:**
The "administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect EPHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

3. **Physical Safeguards:**
The "physical measures, policies, and procedures that protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

4. **Technical Safeguards:**
The "technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

5. **Organizational Requirements:**
The "standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations and requirements for group health plans."

6. **Policies, Procedures & Documentation Requirements:**
The "implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Security Rule; maintenance of written (which may be electronic) documentation and/or records that includes policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation."

Vulnerability Assessments & How to Help Ensure Compliance

The HIPAA Security Rule helps enforce effective risk management to protect EPHI. However, the challenge remains: how do administrators ensure there are zero security holes and that every single device is HIPAA compliant?

Vulnerability Assessments provide the knowledge to understand and respond to the latest cyber threats. Healthcare administrators can audit information systems, assess remediation plans, and acknowledge ongoing security compliance using enterprise-grade vulnerability assessments deployed from a global cloud management console by utilizing infrastructure scans through the secure, convenient CES portal. Once evaluations are concluded, teams can view technical and executive reports within the secure portal.

Benefits

CES' Vulnerability Assessment helps healthcare facilities harmonize a process to fully fortify their network infrastructure by determining and prioritizing vulnerabilities on an infrastructure level and delivering the recommended remediation actions.

Simplified Vulnerability Management

Quick service enabling, continuous vulnerability evaluations, dynamic risk prioritization, simplified remediation action implementation

Regulation Compliance

Supports PCI, NIST, SANS, Mitre Att&Acc

Scalable

Manages high-volume asset scanning

24/7 Coverage

Service operated by certified, highly-trained cybersecurity experts

Internal Scanning Probes

Secure services enabled from cloud management console and internal scanning probe(s)

Remote Implementation

Client-provided server to allow for remote implementation of the probes

Comprehensive Scanning Events

Detailed scanning event(s) requests managed through the CES service portal

info@usclaro.com
Vulnerability Assessment
833-992-5276

Claro Enterprise Solutions