HIPAA Security Risk Analysis

are you compliant...

An annual HIPAA Security Risk Analysis is required by the U.S. Department of Health & Human Services (HHS), as defined by the HIPAA Security Rule. The Security Rule requires organizations to "implement policies and procedures to prevent, detect, contain, and correct security violations."

The HHS Office for Civil Rights (OCR) has also begun its next phase of audits. The 2016 Phase 2 HIPAA Audit Program will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security and Breach Notification Rules.

The team at vcpi provides you with senior level HIPAA security expertise, decades of experience with LTPAC /senior living, and the technical capability to enforce, report and manage security controls. Our HIPAA Security Risk Analysis is a focused review that covers all Standards and Implementation Specifications in the HIPAA Security Rule as well as requirements related to the HITECH Act Breach Notification rules.

The analysis assembles a baseline set of security controls that are applicable to all healthcare organizations. You'll receive a specialized baseline analysis that can fulfill your "Risk Analysis" HIPAA requirement when performed annually. You'll also receive a scorecard and report of all findings, and we'll include remediation recommendations for any issues that are discovered.

Additionally, we've partnered with Compliancy Group, a compliance leader not only in achieving HIPAA, HITECH and Omnibus Compliance for its clients, but also with a 100% success rate in passing compliance audits. You too can gain the HIPAA Seal of Compliance by utilizing The Guard, an advanced web-based solution that helps you achieve, illustrate and maintain compliance year after year.

our process includes...

- **Collect and review your existing security documentation (e.g., policies, standards, procedures, etc.)**
- **Conduct interviews with personnel from your Financial, Human Resources, IT and Nursing teams**
- **Coordinate discussions with your representatives who have knowledge of the security control environment**
- **Schedule the onsite evaluation of your facility(ies) and your associated security control processes**
- **Assemble materials necessary to test the effectiveness of the assessed controls**
- **Analyze collected data, compile analysis findings and assign risk ratings**
- **Present scorecard, analysis report and any remediation plan recommendations**

HIPAA Security Risk Analysis

vcpi

security categories addressed...

General Information Security

- Information Security Governance

Organizational Security

- Vendors and Related Third-Party Agreements
- Assignment of Information Security Responsibility

Information Assets Privacy & Security

- Secure Handling/Storage of Confidential Information
- Secure Information Exchange/Transmission
- Data Destruction
- Security of Unattended Equipment

Physical & Environmental Security

- Physical Access Controls for Facilities
- Visitor/Contractor/Third-Party Access
- Environmental Protections
- Maintenance Records

Network Operations Security

- Encryption
- System Audit Logging and Monitoring
- Security Control Testing
- Information Backups
- Equipment & Software Inventory
- Equipment Transportation

Network Operations Security (cont.)

- Anti-Virus/Malware
- Intrusion Protection/Detection Systems
- Vulnerability/Patch Management
- Firewalls
- Network Segregation

Logical Access Security

- User Access for Network and Systems
- User IDs
- Passwords
- User Sessions

Systems Development & Change Management Security

- Systems Development
- Change Management

Business Continuity/Contingency Operations

- Business Continuity Plan
- Plan Testing and Personnel Training
- Business Impact Analysis
- Disaster Recovery Plan
- Contingency Operations for Emergency Situations