# HIPAA security risk analysis

## Guard against HIPAA violations

We can help your organization measure its current compliance levels and get ahead of the game when it comes to HIPAA audits. 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.

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 "[i] mplement policies and procedures to prevent, detect, contain, and correct security violations."

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

1. Collect and review your existing security documentation (e.g., policies, standards, procedures, etc.)
2. Conduct 15 to 30 minute interviews with personnel chosen from your Financial, Human Resources, IT, and Nursing staff
3. Coordinate thorough discussions with your representatives who have knowledge of the security control environment
4. Schedule the onsite evaluation of your locations and associated security processes (where applicable)
5. Assemble materials necessary to test the effectiveness of the assessed controls (where applicable)
6. Analyze collected data, compile analysis findings and assign risk ratings
7. Present scorecard, analysis report and any remediation plan recommendations

# HIPAA security risk analysis

## Security categories addressed

The following is a high level overview of the security information discussed and documented as part of our analysis; these security categories are mapped directly to the HIPAA Security Rule, as well as other related industry best practices.

### 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
- 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