



HIPAA Security Risk Assessments

Healthcare Providers & Business Associates

Security Risk Assessments

Compliance with the Health Insurance Portability and Accountability Act (HIPAA) and HITECH means taking real actions to address the privacy and security of Protected Health Information (PHI) and then documenting those specific actions as required by the regulations. A security breach or data loss can put a healthcare provider at risk of fines and enforcement actions by HHS and the Office of Civil Rights (OCR) .

A Security Risk Assessment performed by HIPAA Solutions, LC can assist in identifying vulnerabilities in the network and IT infrastructure of a healthcare provider or business associate. As part of the assessment, we will provide recommendations and remediation strategies that can assist in preventing breaches and data loss.

If an organization experiences a security or privacy breach involving PHI, it is critical that legally required mitigation actions be taken immediately.



Security Risk Assessment Resources

- IT Infrastructure - servers and operating systems
- Network Infrastructure – routers, firewalls, workstations and e-mail systems
- Internal and external network system
- User access - online applications or PHI in records
- Business processes and computer applications
- Compliance status related to the “minimum necessary” rule of HIPAA
- Meaningful Use Risk Assessments
- Policies and procedures relating to specific job functions & departments
- Analysis of documentation of implementation as proof of compliance for all HIPAA / HITECH legal and technical mandates
- Tracking / documentation of access and use of PHI

IS YOUR ORGANIZATION COMPLIANT WITH HIPAA?

How have you ensured that your office is complying with the Privacy and Security rules of HIPAA?

Did you do an in depth audit of the organization and apply the minimum necessary rule to job functions?

If your office applied for “Meaningful Use” status for electronic health record funds, did you conduct the Security Risk Assessment of your network and IT environment required for approval of MEU?

What type of documentation do you keep on your compliance activities in the event of an audit?

How do you manage the accounting of disclosures for transactions involving PHI?

Do you keep policies, procedures and training updated to ensure they are in compliance with the current regulations and the Omnibus Rule?

In the event of a government audit, would you be able to quickly provide any required information?

If you need help with HIPAA compliance, contact HIPAA Solutions, LC today to learn about the cost-effective tools and resources that make compliance easier and reduce the risks of non-compliance.

HIPAA Solutions, LC

Toll Free Phone: (877)-779-3004

Web: www.hipaasolutions.org

Email: info@hipaasolutions.org