HIPAA Risk Assessment

Scope & Deliverables

A HIPAA risk assessment measures the level of compliance of a covered entity's policies and systems with the HIPAA Security Rule and HIPAA Privacy Rule and identifies potential risks and vulnerabilities to the confidentiality, availability and integrity of any personal health information (PHI) that the entity creates, receives, maintains, or transmits. HIPAA risk assessments should be periodically reviewed and depending on the circumstances may be conducted annually.

To achieve these objectives the HIPAA Risk Assessment will:

- Identify where PHI is received, maintained, transmitted or stored.
- Identify and document potential threats and vulnerabilities.
- Assess current security measures used to safeguard PHI.
- Assess whether the current security measures are used properly.
- Determine the likelihood of a "reasonably anticipated" threat.
- Determine the potential impact of a breach of PHI.
- Assign risk levels for vulnerabilities.
- Document the assessment and act where necessary.

HIPAA Assessment Process

1. Review existing HIPAA policy and procedures
2. Inspect physical security controls
3. Inspect technical security controls
4. Inspect administrative security controls
5. Deploy tools and conduct internal vulnerability and infrastructure compliance scans
6. Conduct cloud based external vulnerability scan

HIPAA Assessment Deliverables

- ✓ Executive Summary
- ✓ Detailed Vulnerability Report
- ✓ Infrastructure compliance reports
- ✓ Compliance Assessment Report
- ✓ Prioritized Remediation Plan
- ✓ Remediation Services

MAINSTREAM
TECHNOLOGIES

info@mainstream-tech.com / 1-800-550-2052