

## SECURITY RISK ANALYSIS FOR 'MEANINGFUL USE'

“Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process”

--CMS Meaningful Use Rule, Core Menu Set

### Security Risk Analysis:

Security Risk Analysis, the fundamental tenet for HIPAA and HITECH, is also the primary component for Privacy & Security requirements under Meaningful Use. It is essential that risks are identified and prioritized in terms of likelihood of occurrence and impact to the organization so that mitigation strategies can be deployed. The HHS Office of Civil Rights (OCR) guidance document published July 2010 on conducting a HIPAA Risk Analysis stipulates that the risk analysis is foundational and must be fully understood before it can be determined which safeguards and technologies will best protect PHI--Protected Health Information.

### OCR's Elements of a Risk Analysis from

#### “Guidance on Risk Analysis Requirements under the HIPAA Security Rule”

“There are numerous methods of performing risk analysis and there is no single method or “best practice” that guarantees compliance with the Security Rule.” Here are “several elements a risk analysis must incorporate, regardless of the method employed.”

- 1. Scope of the Analysis:** “The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).)”
- 2. Data Collection:** “An organization must identify where the e-PHI is stored, received, maintained or transmitted. An organization could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques.”
- 3. Identify and Document Potential Threats and Vulnerabilities:** “Organizations must identify and document reasonably anticipated threats to e-PHI.”
- 4. Assess Current Security Measures:** “Organizations should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly.”
- 5. Determine the Likelihood of Threat Occurrence:** “The Security Rule requires organizations to take into account the probability of potential risks to e-PHI.”
- 6. Determine the Potential Impact of Threat Occurrence:** “The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of e-PHI.”
- 7. Determine the Level of Risk:** “Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis.”
- 8. Finalize Documentation:** “The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).) The risk analysis documentation is a direct input to the risk management process.”
- 9. Periodic Review and Updates to the Risk Assessment:** “The risk analysis process should be ongoing. In order for an entity to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed.”

## **Three Phases of the BluePrint Security Risk Analysis for ‘Meaningful Use’:**



### **Phase One: Digital Binder Review**

1. Policy and Procedures
2. Security & Privacy Program Management Documentation
3. Previous Security Audits and Risk Assessments
4. Current Security, Privacy, Access and Audit Controls
5. Data Breach and Incident Response Procedures
6. Disaster Recovery and Business Continuity Documents
7. Business Associate Agreements
8. Information Lifecycle Documentation

### **Phase Two: Comprehensive Security Assessment Program**

1. Physical Security Walk-throughs
2. Information Lifecycle Walk-throughs
3. Security Assessments of Primary Clinical Applications
4. Security Assessments of Key Departments
5. Evaluate Security Controls and Vulnerabilities

### **Phase Three: Security Risk Analysis and Remediation Roadmap**

1. Identify Security & Privacy Gaps
2. Assign Impact and Probability Risk Ratings
3. Identify Remediation Recommendations
4. Implementation Roadmap

### **Information Security Advisor:**

As part of the Security Risk Analysis for ‘Meaningful Use’, BluePrint provides an information security advisor for the entire engagement to work with your organization or committee. The Advisor serves as the focal point for the engagement, coordinates activities, provides guidance, and identifies critical issues during any phase of the process.

*BluePrint Healthcare IT is a recognized leader in healthcare IT security, privacy, compliance and risk management. BluePrint S-PAC (Security, Privacy and Compliance) Services for hospitals, healthcare systems, and health information exchange reduce an organization’s risk exposure. S-PAC Services are designed to allow clients to engage BluePrint for the development, execution and management of security and risk mitigation programs. Advisors and Analysts work with the client’s staff to deliver secure, compliant and meaningful solutions.*



Scan with Smartphone  
for more information.

Vikas Khosla  
President & CEO  
[vikas.khosla@blueprinthis.com](mailto:vikas.khosla@blueprinthis.com)  
732.690.0885

Gregory Michaels  
Director, Security & Compliance Solutions  
[greg.michaels@blueprinthis.com](mailto:greg.michaels@blueprinthis.com)  
732.910.3751

Mike Squires  
Vice President Strategic Development and  
Public Policy  
[mike.squires@blueprinthis.com](mailto:mike.squires@blueprinthis.com)  
908-391-6191

**BluePrint Healthcare IT**, Cranbury Executive Center, 1249 South River Road, Suite 106, Cranbury, NJ 08512  
732.607.0011 [www.blueprinthis.com](http://www.blueprinthis.com)