HIPAA Privacy & Security Risk Assessment

Background

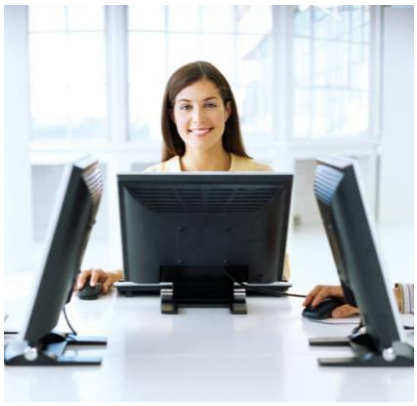
The American Recovery and Reinvestment Act (ARRA) of 2009 includes the Health Information Technology for Economic and Clinical Health (HITECH) Act.

ARRA describes "improvements" to existing HIPAA laws, covered entities, business associates, and others who will be subject to more rigorous standards when it comes to protected health information (PHI).

The HITECH Act expands the scope of the HIPAA Privacy and Security Rules and increases the penalties for HIPAA violations.

Specifically, the HITECH Act addresses 5 main areas of the HIPAA regulations.

- *Applies the same HIPAA privacy and security requirements (and penalties) for **covered entities** and **business associates***
- *Establishes mandatory federal privacy and security breach reporting requirements for HIPAA covered entities and business associates*
- *Creates new privacy requirements for HIPAA covered entities and business associates, including new accounting disclosure requirements and restrictions on sales and marketing*
- *Establishes new **criminal** and **civil penalties** for HIPAA non-compliance and new enforcement methods*
- *Mandates that the new security requirements must be incorporated into all Business Associate contracts*



Whether a healthcare organization striving for Meaningful Use dollars, or simply a business associate handling protected health information (PHI), the Department of Health and Human Resources (DHRR) requires organizations demonstrate they keep PHI data secure during storage, during transmission, and while it is being used.

45 CFR§164.306(a)(1) *"Covered entities and business associates must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits."*

In addition, covered entities, and business associates, are also **required to conduct a risk assessment** to identify all risks and vulnerabilities that may contribute to a PHI breach.

45 CFR§164.308 (a)(1)(ii)(A) "*A covered entity, or business associate, must: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."*

**It is important also to note the American Recovery and Reinvestment Act (ARRA) created civil fines and penalties for HIPAA violations ranging up to $50,000 per occurrence, depending on the type, and level, of violation. However, if there is willful neglect, the penalty is $50,000. The criminal penalties can range up to $1.5 million and 10 years imprisonment.

Assessment Process

The process follows eight specific steps:

1. Identify and collect the data
2. Identify and document the threats and vulnerabilities
3. Assess the current level of security
4. Make a determination of the threat probability
5. Determine the potential impact of each threat
6. Assign specific risk levels for each threat and vulnerability
7. Determine recommended remediation steps
8. Document in final report (Deliverable)

The Proj*X* Privacy & Security Risk Assessment concentrates on four key areas, mentioned in the HIPAA requirements, as it goes through each of the steps mentioned above.

1.	Physical	45CFR§164.310
2.	Technical	45CFR§164.312
3.	Organizational	45CFR§164.314
4.	Administrative	45CFR§164.316

In addition, the Proj*X* Privacy & Security Risk Analysis also goes into great depth identifying threats and vulnerabilities within the IT arena. To this end, we perform a very detailed **Network & Penetration Testing** on our client's Information Technology Network, *as described on the following page*.

Deliverables

- Current Network Diagram
- Network Vulnerability Outline
- Application Criticality Matrix
- Probable Threat/Impact Matrix (External Issues
- Vulnerability Matrix (Internal Issues)
- Comprehensive ePHI Inventory
- Security Risk Matrix (Listed by Risk Severity)
- Remediation Recommendations

ProjX Incorporated