HIPAA SECURITY RISK ANALYSIS

HIPAA covered entities that have access to ePHI must conduct a security risk analysis as part of their HIPAA management processes. HIPAA does not require that specific security measures be taken by every covered organization. Rather, the covered entity should conduct a risk analysis and implement appropriate security measures based on its specific situation. The risk analysis process includes, but is not limited to:

- Evaluation of the type of PHI received, created, maintained or accessed by the covered entity, and the flow of that PHI through the entity;
- Evaluation of the likelihood and impact of potential risks to e-PHI;
- Implementation of appropriate security measures to address the risks identified in the risk analysis;
- Documentation of the chosen security measures and, where required, the rationale for adopting those measures; and
- Maintenance of continuous, reasonable, and appropriate security protections.

In particular, after identifying the type of ePHI received, created, maintained or accessed by the Plan, and the potential or risk of non-authorized access to or disclosure of such information, the risk analysis should consider the type of safeguards needed to protect the e-PHI. The three types of safeguards that should be considered include:

Administrative Safeguards

Security Management Process. As explained in the previous section, a covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

Security Personnel. A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

Information Access Management. Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).

Workforce Training and Management. A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Evaluation. A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

Physical Safeguards

Facility Access and Control. A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.

Workstation and Device Security. A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

Technical Safeguards

Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

Audit Controls. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

Integrity Controls. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.