Securing Protected Health Care Information (PHI)

Introduction
The technical practices and procedures section of the Health Care Information Portability and Accountability Act (HIPAA) requires health care organizations to deploy systems for individual authentication of users, to install access controls and maintain audit trails, to implement physical security and disaster recovery, to protect remote access points and electronic communications, and to perform a full HIPAA/HITECH Compliance and Network Security Audit.

HIPAA mandates security however it does not give specific information on how security should be implemented within an organization. For example, health care employees must have a user name and password to access patient information and that data must be encrypted when it leaves a health care organization's network. However, it is up to each individual health care organization to determine the password strength and level of encryption required.

Health Information Technology (HIT) Challenges
Health Information Technology (HIT) provides many benefits, but presents many challenges. Securing electronic patient information prevents health care organizations with many challenges. Some of these challenges include:

- Connecting people with information. The secure sharing of patient information among multiple health care providers and payers is a challenge. By aggregating a patient's health information, organizations need to be concerned about privacy and security.
- Policy. In many health care organizations, there is no straightforward structure with one person that can dictate and manage policy. As a result, many organizations have security solutions that are ad-hoc and not properly aligned.
- Budgets and funding. Without top-down support from management, organizations may not allocate sufficient funds to security related areas.
- Electronic Medical Records (EMR). EMR systems such as eClinical Works, Allscripts, Medical Communications Systems, and Practice Partner automate scheduling, charting, patient flow, billing, and messaging. However not every package has the level of security and functionality needed. As health care organizations implement EMR systems, they find that integrating HIPAA and EMR can be difficult.

Risk Management
Many health care organizations don't know how to complete a solid risk assessment and then create a risk management plan that meets the requirements of HIPAA and the Information Systems Audit and Control Association (ISACA).

The objective of risk management is to enable the organization to accomplish its mission:

- By better securing the IT systems that store, process, or transmit organizational information
- By enabling management to make well-informed risk management decisions
- By justifying the expenditures that are part of an IT budget

The three steps to risk management include:

- Risk assessment – identify assets and threats to the assets.
- Risk analysis – identify likelihood and impact of the event.
- Risk treatment – identify preventive, detective, and corrective controls that treat risks.

Mitigating Risks

Once risks have been identified by an assessment, health care organizations have many options to mitigate the risks:

- Risk Assumption. Accept the potential risk and continue operating the IT system or implement controls to lower the risk to an acceptable level. Administrative, physical, and technical controls help lower the organization's risks.
- Risk Avoidance. Avoid the risk by eliminating the risk and/or consequence. For example, bypass or eliminate certain functions of a system or shut down the system when risks are identified.
- Risk Limitation. Limit the risk by implementing controls that minimize the adverse impact of the risk. For example, implement preventive controls such as Intrusion Prevention Systems (IPS) that actively identify and restrict access to information.
- Risk Planning. Manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls. Implement managed services to minimize risks.
- Risk Research. Lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
- Risk Transference. Compensate for the loss by transferring the risk to another party. In addition to securing systems, health care organizations have the option to insure against security breaches. For example, insurance can cover the cost of regulatory mandated notifications that a security breach has occurred as well as fines, fees, or penalties arising from privacy or consumer protection errors.

Network security audits review administrative, physical, and technical safeguards and controls to ensure they are sufficient and effective at protecting information systems and PHI.

Summary
Securing electronic patient information requires physician groups, hospitals, ambulatory surgery centers, health care data processors, health care software providers, image delivery systems, long-term care facilities, and managed care organizations to proactively implement administrative, physical, and technical controls.

Each health care organization has a unique environment that makes it difficult to comply with HIPAA's regulations. Network and security assessments help organizations meet compliance requirements by identifying, managing, and reducing their risks.

Publication Information
Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.