HIPPA Whitepaper

Information Exchange Systems and Synergy IXS are committed to protecting the privacy of individual's personal health information. Part of this commitment is strict compliance with the Privacy Rule of the Health Portability and Accountability Act of 1996 (HIPAA), which requires us to take additional measures to protect personal information.

How do IXS systems and processes comply with HIPAA?
We have established a HIPAA Security Rule, which applies to health information maintained or transmitted by a Covered Entity in electronic form. This information requires administrative, physical and technical protection.

Administrative protections:

- Security management.
- Policies to prevent, detect, contain and correct security violations; risk analysis, risk management, and sanction/security policies.
- Assigned responsibility - single individual must have responsibility, assigned in writing, for the overall security of a covered entity's information.
- Workforce security - only authorized staff may have access to information.
- Information access - policies for authorizing, establishing and modifying access to information.
- Security awareness/training - program for entire staff developed and maintained.
- Security incident procedures - policies are in place to report, respond to and manage security incidents.
- Business Continuity Plan - for response to disaster/emergency that damages information systems containing information.
- Evaluation - periodically determine the extent that our security policies meet the ongoing requirements.
- Business Associate Agreement - states that we will adequately safeguard the information.

Physical protections:

- Facility access - limit physical access to information.
- Workstation use - policy specifies the use of workstations and the characteristics of the physical environment of workstations that can access information.
- Workstation security - limited only to authorized users.
- Equipment controls - for recovered information and removal of hardware and electronic media containing information.

Technical protections:

- Access control - only authorized personnel have access.
- Audit controls - to record and examine activity within systems.
- Integrity - to protect information from improper modification or destruction.
- Person/Entity authentication - to verify that persons seeking access to information are who they claim to be.
- Transmission security - to prevent unauthorized access to information that is transmitted electronically.