

## **IMPLEMENTING HIPAA'S SECURITY RULE STANDARDS AN OVERVIEW FOR OUR MEDICAL STAFF**

The HIPAA Privacy Rule became effective in April of 2003. This was a challenging process as the Rule was comprehensive, complex, and confusing. While we continue to work with patient privacy issues, we now must also focus on compliance to the HIPAA Security Rule which went into effect April 20, 2005. While the Security Rule is not as complex as the Privacy Rule, it does require that we expand our commitment to patient privacy to address protecting the confidentiality, integrity, and availability of our patients' electronic protected health information (ePHI) by establishing:

**Administrative Safeguards:** People, policies, plans and processes are the foundation for Administrative Safeguards. Policies and processes are either in the process of or have been developed to ensure:

- Access to ePHI is controlled and limited to those workforce members who have a need to know.
- Systems are in place to detect, correct, and prevent privacy and security breaches.
- Disaster, business continuity, and contingency planning is addressed and plans developed.
- Ongoing evaluations and audits to determine compliance are carried out.
- Security incidents are identified and responded to appropriately.

**Physical Safeguards:** Physical safeguards address things such as computers, computer applications and systems, equipment, and even the areas where they are stored. Policies and processes are either in the process of or have been developed to ensure:

- Limited physical access to authorized workforce members only.
- Management of workforce members' passwords and unique user ID's.
- Facility access, workstation use and security controls.
- Appropriate destruction, disposal, and reuse of equipment.

**Technical Safeguards:** These safeguards include the technology that Saint Clare's Hospital has in place to protect ePHI. Generally these safeguards are put into place by the Information Services Department and cover:

- Access controls and authentication; internal audits and controls to track and record activity.
- Virus and malicious code prevention.
- Transmission safeguards and encryption.

### **How Will Implementation of the HIPAA Security Rule Impact You and Your Staff?**

- Saint Clare's Hospital will have in place stronger processes to ensure appropriate access to our electronic patient care records, applications, and systems.
- Users of Saint Clare's Hospital's applications and systems will be assigned and expected to use a unique user ID. Generic and shared passwords will be phased out.
- Management of individual passwords will force users of our applications and systems to choose more complex passwords at more frequent intervals.
- A greater emphasis on physical safeguards will lead to increased verification requirements, ensuring that individuals accessing patient ePHI are known (name badges/ID's) and have need-to-know access rights.
- Saint Clare's Hospital will carry out increased auditing of access to determine appropriateness.

### **What Policies Will Be Implemented as a Result of the HIPAA Security Rule?**

In order to ensure compliance with the HIPAA Security Rule, Saint Clare's Hospital has developed policies and procedures that will address:

- Authentication Standards
- Remote Access
- Workforce Use & Security
- E-Mail
- Security Incident Reporting
- Emergency, Contingency, and Disaster Planning

If you have any questions regarding how the Saint Clare's Hospital will address the HIPAA Security Rule or if we can provide assistance to you and your staff in your own implementation efforts, please contact our local Security Officer, Shirley Bailey at 715-346-5291.