GALEN
MEDICAL GROUP

HIPAA Security Awareness

Security Incident Response Procedures

A "Security Incident" is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with Galen's patient information system. Examples Include:

- Computer intrusions
- Unauthorized computer access
- Lost or stolen electronic devices
- Denial of service to authorized users, and
- Administrative and physical incidents such as theft, unlocked doors, unauthorized facility entry, or unauthorized computer access.

Employees must report suspected or known security incidents by:

- Direct verbal report to the Privacy Officer at (423) 762-7075
- If incident involves Galen's electronic information systems, a direct report should be made to the Security Officer at 308-0525, then to the Privacy Officer.
- Reports may be made to your immediate supervisor immediately before or after reporting to the Security Officer and/or the Privacy Officer.

Malicious Software

- Malicious software is
  - Software designed to damage or disrupt a system
  - Software that has an intentional negative impact of the confidentiality, availability, or integrity of PHI
- Malicious software can
  - Destroy your computer files, or
  - Block your access to critical computer applications
- Malicious software includes viruses, worms, and trojans.

Protecting Against Malicious Software

- Approved anti-virus software must be installed and kept current on all computer systems.
- Never disable anti-virus software.
- Suspicious software should be brought to the attention of the IT technical support personnel immediately.
- Suspicious e-mails or file attachments should not be opened.

Password Management

- Your user ID and password are critical to ePHI security.
- Maintain your password in a secure and confidential manner.
  - Do not share your password with anyone
  - Passwords must be changed every 90 days
  - Strong passwords must be utilized when possible
  - Your are personally responsible for access to any information utilizing your password

Log-In Monitoring

- The Security Officer will monitor logon attempts to Galen's network.
- Inappropriate logon attempts should be reported to the Security Officer at 308-0525
- All Galen computer systems are subject to audit.

Facility Security

- Galen identification badges should be worn at all times while at any Galen clinical facility.
- The reception area must be staffed at all times during site office hours.
- Entrance to clinic areas must be locked and/or supervised for authorized access.

Electronic Media Care, Electronic Disposal or Reuse

- Electronic media or devices containing ePHI may not be reused or removed from Galen sites without proper authority.
- Such media or devices may be reused or destroyed only by authorized persons following approved procedures.
- Before any electronic media or device is permanently removed from a secure Galen site, the entire media or device must first
  - be overwritten with a minimum of three passes, or
  - be physically destroyed by shredding, pulverizing, or incineration, and
  - the time, date and circumstances must be documented.
- Any data storage device may be removed temporarily from Galen sites only if
  - the ePHI is fully encrypted to appropriate encryption standards, and
  - the device is entrusted to an authorized employee or business associate.

Workstation Security

- Workstations and applications shall be monitored for unauthorized use, tampering, and theft.
- To the extent space may practically allow, workstations should be positioned so as to avoid viewing by unauthorized personnel.
- Use of automatic password protected screen savers should be utilized.
- Lock, logoff, or shut down workstations when left unattended.

Contingency Plan

- A system must be in place to ensure recovery from any damage to computer equipment or data within a reasonable time period.
- A copy of Galen's Contingency Operations Plan may be obtained from the Site Manager.
- Galen's Contingency Operations Plan includes:
  - Data Backup Plan
  - Disaster Recovery Plan
  - Emergency Mode Operations Plan
  - Testing and Revision Procedures