GOOD SAMARITAN HEALTH AND WELLNESS CENTER

POLICIES AND PROCEDURES

Subject: Security Awareness and Training	Policy #: 4.9.16
Prepared by: Teri Craig	Effective Date: 07/15/2016
Approved by: Board	Revision Date:

PURPOSE:

To establish a security awareness and training program for all members of Good Samaritan Health and Wellness Center's workforce, including management.

POLICY:

All Good Samaritan Health and Wellness Center employees/volunteers shall receive appropriate training concerning GSHWC's security policies and procedures. Such training shall be provided on an ongoing basis to all new employees/volunteers. Such training shall be repeated annually for all employees/volunteers.

PROCEDURE:

A. Security Training Program

- The Security Officer along with assistance from the IT department shall have the responsibility for the development and delivery of initial security training. All employees/volunteers shall receive said initial training addressing the requirements of the HIPAA Security Rule, including the updates to HIPAA regulations found in the Health Information Technology for Economic and Clinical Health (HITECH) Act. Security training shall be provided to all new employees/volunteers as part of the orientation process. The Security Officer shall be responsible for maintaining appropriate documentation of all training activities.
- The Security Officer along with assistance and guidance of the IT department shall have responsibility for the development and delivery of ongoing security training provided to employees/volunteers in response to environmental and operational changes impacting the security of ePHI (new hardware, new software, and increased threats).

B. Security Reminders

- The Security Officer shall generate and distribute to all employees/volunteers routine security reminders on a regular basis as deemed appropriate by the IT department. Periodic reminders shall address password security, malicious software, incident identification and response, and

access control. The Security Officer may provide such reminders through formal training, e-mail, discussions during staff meetings, log-in banners, etc.

- The Security Officer shall generate and distribute special notices providing urgent updates such as new threats, hazards, vulnerabilities, and/or countermeasures.

C. Protection from Malicious Software

- The Security Officer with the assistance of the IT department shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:
  - Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mails.
  - The importance of updating anti-virus software on individual workstations to keep current.
  - Never download files from unknown or suspicious sources.
  - Recognizing signs of potential viruses.
  - The importance of backing up critical data on a regular basis and storing the data in a safe place.
  - Damage caused by viruses and worms, and what to do if one is detected

D. Password Management

As part of the Security Training Program and Reminders, the Security Officer shall provide training concerning password management in accordance with Good Samaritan Policy 4.9.3, “Password Management Policy”.