Good Samaritan Health and Wellness Center

Policies and Procedures

Subject: Wireless Security	Policy #: 4.9.4
Prepared by: John Hilliard	Revision #:
Approved by: Board of Directors	Effective Date: 4/22/2016

4.9.4 Wireless Security

PURPOSE

This policy has been implemented in order to protect the confidentiality, integrity, and availability of the **Good Samaritan Health & Wellness** wireless network infrastructure and data from being compromised through the unauthorized exploitation of wireless network access technology.

SCOPE

The policy applies to **Good Samaritan Health and Wellness Center** facilities as well as any devices attached to the **Good Samaritan Health and Wellness Center** network.

POLICY

- The deployment and use of open, unsecured wireless network access for **Good Samaritan Health and Wellness Center** business functions is prohibited.
- Before introducing or modifying any wireless access technology, the Security Officer must conduct an assessment and review of the information security risks entailed.
- The organization's Security Officer shall conduct periodic reviews, including penetration tests and vulnerability assessments, to ensure that wireless network access is deployed securely and in compliance with all applicable established standards.
- **Good Samaritan Health and Wellness Center** will implement the most secure and reasonable wireless security available.
- The operation and use of wireless access technology will comply with all HIPAA policies and procedures applicable to wireless information security.
- Authentication should force potential clients to authenticate themselves to the network before connection (Shared Key Authentication). Access points will be sited so as to minimize signal radiation outside the building. The Service Set Identifier (SSID) shall in no way identify the agency, and default SSIDs shall not be used.

- Security awareness and training shall specifically inform users of the risks of using mobile and wireless technology, and inform them of the most secure methods of using this technology.

VIOLATION REPORTING

Any observed misuse or violation of this policy should be immediately reported to one of the following persons:

- Executive Director,
- Chief Financial Officer,
- Security Officer

DEFINITIONS

HIPAA – The Health Insurance Portability and Accountability Act of 1996 (HIPAA) which required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy (Privacy Rule) and security (Security Rule) of certain health information.

Personal Health Information (PHI) – Individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Virtual Private Network (VPN) – A secure connection to a private network created on the public telecommunication infrastructure or Internet.