Silverton Hospital Network
GENERAL MANUAL

TITLE: **INFORMATION PRIVACY & SECURITY**	**PAGE: 1 of 4** **Policy No: GEN-IM-141**

Date Issued: April 2002	**Source/Reference:** Joint Commission, Standard IM.02.01.01, IM.02.01.03,IM.03.01.01
Date Reviewed: May 2006, December 2009	
Date Revised: December 2009	**Departments Affected:** All
Author: IS Director	

PURPOSE: Consistent with our Mission Statement and Values, Silverton Hospital Network (SHN) strives to ensure an ethical and compassionate approach to healthcare delivery and management. SHN recognizes the importance of preserving privacy. Furthermore, protecting the integrity of information is essential.

- Information and information systems are critical and vitally important SHN assets. Information security refers to preserving the confidentiality, protecting the integrity, and ensuring the availability of information.
- To be effective, information security must be a team effort involving the participation and support of every SHN colleague who deals with information and/or information systems. This means that SHN takes appropriate steps to ensure that information and information systems are properly protected in accordance with internal polices and local, state, and federal laws and regulations.

POLICY STATEMENT: The Silverton Hospital Network Privacy and Security Policy provides guidance to all employees, board members, providers, agents, consultants, volunteers, contractors, and suppliers in carrying out their daily activities. Throughout this document, this group of affected individuals is collectively referred to as "colleagues" of SHN. The obligation under this policy apply to SHN's relationships with patients, volunteers, third party payers, subcontractors, vendors, consultants, Business Associates, and one another.

Access to SHN information and the sharing and security of that information requires that each colleague accept responsibility to protect the rights of SHN. Any user of SHN resources who, without authorization, distributes, accesses, uses, destroys, alters, dismantles, disfigures or disables SHN information resources creates a threat to the secure environment of SHN. These actions are subject to discipline under the Information Services Violation Policy.

PROCEDURE:

1. In the course of business, it is necessary for SHN to record, store, process, transmit, and otherwise handle private information about individuals and employees. SHN takes these activities seriously and seeks to provide fair, secure, and legal systems for the appropriate handling of this private information. It is the intent of SHN to

provide the policies, procedures, and training necessary to protect the privacy of sensitive information.

2. SHN collects information about patient's medical condition, history, medication and family illnesses to provide the best possible care. SHN does not release or discuss patient-specific information with others unless it is necessary to serve the patient, required by law or considered public information.
3. Confidential information about SHN's strategies and operations is a valuable asset. This information must not be shared with others outside of SHN unless the individual has a legitimate reason to know and agrees to maintain the confidentiality of information.
4. It is critically important to maintain patient confidentiality, as well as to maintain confidentiality about SHN employees and business information. This policy pertains to all information, (verbal, paper, and electronic) related to the operation of SHN including, but not limited to:
   - Patient names and other identifying information.
   - Patient specific health information.
   - Patient billing information.
   - Other personal information related to patients.
   - Employee names, including pay rates and employment information.
   - Marketing and general business strategies.
   - Financial information.
5. In addition to the above, any information that has been marked "confidential" by SHN is deemed to be covered under this policy. Unauthorized access, use, or release of confidential and sensitive information to non-authorized individuals is strictly prohibited and may result in immediate disciplinary action up to and including termination.
6. This policy applies to all SHN subsidiaries, divisions, departments, and organizational units.

Accountability and Responsibility: Maintaining information, privacy, and security is the responsibility of all SHN colleagues. The responsibility includes assuring compliance with SHN's polices for confidentiality by non-SHN employees performing work at, or for SHN. Business Associates, vendors, consultants, and subcontractors working with SHN, must be informed of their obligations regarding SHN information, privacy, and security polices and agree to consequences appropriate to any breach of such polices. Contracts must include language specifying obligations regarding privacy and security and consequences of a breach when appropriate.

<u>User Responsibility:</u> A "user" is any person who accesses any corporate data in any form. Each user is responsible for:

1. Maintaining the confidentiality of information.
2. Complying with SHN policies, standards, and procedures including those in this document.

3. Taking any reasonable and logical measure that is necessary to preserve information confidentiality and privacy even if it is not specifically addressed in a policy.
4. Maintaining a secure work area.
5. Safeguarding output (such as printed reports, screen prints, copies, ancillary storage devices (USB Drives, External Drives, etc)).
6. Reporting an observed or suspected breach of information security to management.
7. Maintaining a secure digital signature.
8. Using only unique system login(s) and not allowing anyone else to use unique system login(s).

<u>Managers/Supervisors are responsible for:</u>

1. Establishing, publishing, and enforcing departmental standards and procedures to:
   a. Prevent unauthorized collection, disclosure, modification or destruction of data.
   b. Develop and maintain data security awareness among subordinates.
   c. Assure that the SHN standards and policies on the length of retention and destruction of information are followed.
2. Reviewing job responsibilities of a new or transferred employee, consultant/ contractor, business associate, or other user, and determining what access to functions/databases is needed to perform their job function.
3. Ensuring requested access is consistent with approved standards.
4. Requesting access by the fewest users necessary to ensure completion of work.
5. IMMEDIATELY notifying Information Services (IS) when a user’s access is terminated.
6. Ensuring staff are updated on SHN’s information security standards/polices.
7. Informing users under their supervision of changes in policies, standards, or procedures.
8. Overseeing their employees’ use of systems, internet and company resources and initiating appropriate disciplinary action.

<u>Information Services is responsible for:</u>

1. Ensuring and maintaining a secured system and network environment.
2. Managing system and network access control.

Access to and Use of Information and Systems: SHN is committed to taking all reasonable and appropriate measures to protect sensitive information against accidental or unauthorized modification, disclosure, or destruction, including the security of the equipment, software, and data. Access to information is only granted on a need to know basis based on role and responsibilities.

1. Computer software, hardware, communication equipment, and encryption capabilities are assets of SHN. All data processing resources (e.g., software, servers, data), owned, used, or maintained by SHN are properly secured in accordance with these standards.
2. Use of SHN computers is primarily for SHN business-related activity or professional development. The electronic environment is part of the workplace and carries with it the same expectation of mutual respect and confidentiality that applies to all other activities at SHN.
3. SHN may use human or automated means to monitor the use of systems handling SHN information. Tools for monitoring or observation of computer user activities may be used with or without prior notification. The findings may be disclosed to management or law enforcement during the course of investigation.

Personal Obligation to Report: All employees or colleagues of SHN, have a responsibility for reporting activity by any employee, physician, volunteer, subcontractor, business associate or vendor that appears to violate applicable laws, rules, regulation, or information privacy and security policies. Failure to do so could serve as a basis for disciplinary action.

Compliance: Failure to comply with confidentiality and information security policies, standards, and procedures may result in disciplinary action which includes termination or suspension of network access. Compliance means conformity to information security policies and standards as well as the information security procedures developed to meet user needs.

1. Managers have the primary responsibility for enforcing and monitoring compliance. Additional support for overseeing compliance is provided by Information Services.
2. Observance of information security polices, standards, and procedures is a condition of employment/participation in SHN's network.

Approvals: Policy Review Team 12/18/09, Vice Presidents 12/18/09

Related Policies: Network & Computer Access GEN-IM-143, Computing Resources GEN-IM-137, Electronic Communication GEN-IM-139