Samaritan Health Services	[X] Corporate [X] GSRMC [X] SAGH	[X] SLCH [X] SNLH [X] SPCH

Policy & Procedure

Page 1 of 7	Revision #: 6
Owner: Information Services	Authorized by: SHS Compliance Committee

Workforce Information Technology Use

APPLICATION

All Samaritan Health Services (SHS) Workforce Members.

POLICY

Workforce Members who use SHS information technology are required to use those resources within SHS-defined limits. Workforce Members must protect the security, availability, confidentiality, and integrity of these information resources and any SHS information assets stored, processed or transmitted. A workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

PROCEDURE

DEFINITIONS:

1. Information resources/Information technology: All SHS information technology, including, but not limited to:
    a. Computing equipment and services
    b. Data storage
    c. Network equipment and services
    d. Software
    e. Peripheral devices installed on SHS IS network or facilities or otherwise furnished by SHS, whether owned, leased operated, or controlled by SHS.
2. Information asset: A definable piece of data stored in any manner that is recognized as 'valuable' to the SHS organization.
3. Protected Health Information (PHI): Information – in any form or media – that is created, stored, or transmitted by SHS, or by an SHS Business Associate, that could reasonably be used to identify the Individual (i.e. an SHS patient or member) AND relates to one of the following:
    a. The Individual's past, present or future physical or mental health or condition;
    b. The provision of health care to the Individual
    c. The past, present or future payment for health care services provided to the individual

    Common examples of PHI include, but are not limited to: name (including first and/or last); mailing address (complete or partial, including zip code); email address; phone or fax number; biometric data including full-face photographs; date of birth, date of death, date of service, or any other date pertaining to the provision of care to a patient or member; and medical record number, member ID number, visit number, social security number, or any other unique identifying number.

In general, the above information is NOT considered PHI if it is held by SHS strictly in its capacity as an employer (such as most SHS employee health records).

4. Personally Identifiable Information (PII): Information – in any form or media – that is created, stored, or transmitted by SHS, or by an SHS Business Associate, that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an Individual in context
5. SHS Guest Network: A wired and/or wireless network, provided by SHS, that allows guests to access the Internet while remaining isolated from the SHS Production Network. Guests are not required to authenticate on the SHS Guest Network.
6. SHS Production Network: The computing environment that is available to Workforce Members through either an SHS-provided physical or wireless connection. Workforce Members must authenticate on the SHS Production Network using their SHS user name and password, their badge, or some other approved unique identifier.
7. User Authorities: Individuals or entities within SHS with user oversight responsibility. Typically, these are personnel managers who are responsible for requesting appropriate role-based access for their employees.
8. Workforce member: any employee, contractor, vendor, volunteer, trainee, and other person whose conduct, in the performance of work for SHS, is under the direct control of SHS, whether or not they are paid by SHS.

IMPLEMENTATION:

1. General Use
    a. The use of SHS information assets and resources is granted based on user understanding and acceptance of this policy.
    b. Workforce Members are required to promptly report the theft, loss, or unauthorized disclosure of SHS information resources and assets.
    c. Except as noted below, Workforce Members may access, use, or share SHS information assets only to the extent it is authorized and necessary to fulfill assigned job duties.
    d. SHS owns the rights to all data and files on any computer, network, or other information system used by SHS and to all data and files sent or received using any SHS system or using the access to any SHS computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property.
    e. SHS reserves the right to monitor electronic mail messages (including personal, private, and instant messaging systems) and their content, as well as any and all use by SHS Workforce Members of the Internet and of computer equipment used to create, view, or access e-mail and Internet content. Employees must be aware that the electronic mail messages sent and received using SHS equipment or SHS-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by SHS officials at all times.
    f. SHS has the right to inspect any and all files stored in private areas of the SHS network or on individual computers or storage media in order to assure compliance with SHS policies and state and federal laws. No SHS workforce member may access another workforce member's computer, computer files, or electronic mail messages without prior authorization from either the workforce member or an appropriate SHS official.
    g. SHS uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that

is entered into, received by, sent, or viewed on such systems. There is no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with SHS equipment or Internet access.

h. SHS Workforce Members should assume that whatever they do, type, enter, send, receive, and view on SHS electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and SHS use at any time. Further, Workforce Members who use SHS systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure.
i. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than SHS systems or the SHS-provided Internet access.
j. SHS has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software.
k. Workforce Members must ensure that computer workstations are placed so that electronic PHI and other sensitive information on the computer screen cannot be read or viewed by unauthorized individuals.
l. Workforce Members must lock the computer screen, log off the computer, or log out of the application they are using (if using a kiosk computer) when the computer is unattended.

2. Internet usage:
    a. While logged on to the SHS Production Network, Workforce Members may use the Internet for business-related purposes, e.g., to communicate with other professionals, to research relevant topics, and to obtain useful business information.
    b. Workforce Members must exercise caution when using the Internet on the SHS Production Network and whenever possible limit their use to business-related purposes. SHS Workforce Members should use personal devices to conduct personal Internet activity. Any personal use of the Internet must be conducted on the workforce member's own time, i.e., during rest breaks and meal periods.
    c. Workforce Members are required to conduct themselves professionally and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and opinions of others. This applies to use of the Internet on both the SHS Production and SHS Guest Networks.
    d. SHS uses independently-supplied software and data to categorize Internet sites when Workforce Members use the Internet on the SHS Production Network. SHS allows or blocks access from within the SHS Production Network to Internet sites based on site categories. For example, SHS blocks access to all websites that are categorized as the following:
        i. Adult Material
        ii. Gambling
        iii. Games
        iv. Illegal or Questionable
        v. Militancy and Extremist
        vi. Personal Network Storage and Backup
        vii. Personal Webmail
        viii. Social Media
        ix. Violence
        x. Weapons

e. SHS Workforce Members who need to access a blocked website for approved business use cases must submit a request to the IS Service Desk. All requests are reviewed by one or more representatives from the SHS Legal, Compliance, and IS Security teams.
f. SHS Workforce Members may not bypass or attempt to bypass the Internet content filters while on the SHS Production Network.
g. SHS has software and systems in place that monitor and record all Internet usage on the SHS Production Network. No Workforce Members should have any expectation of privacy as to Internet usage while on the SHS ProductionNetwork.
h. Employees are prohibited from disclosing PHI, PII, sensitive corporate data, and/or any other material covered by existing SHS policies and procedures on Social Media, chat rooms and newsgroups, and other public forums made available on the Internet.

3. Unacceptable Use: The activities listed below are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). The list of activities is by no means exhaustive, but is rather an attempt to provide a framework for activities that fall into the category of unacceptable use.

   SHS Workforce Members are prohibited from the following:

   a. Connecting personal devices to the SHS network, unless given specific approval from an SHS user authority. These devices include, but are not limited to:
      i. Laptop or tablet computers
      ii. Desktop computers
      iii. Smart phones
      iv. Portable hard drives
      v. Universal Serial Bus (USB) Storage Devices (also commonly referred to as thumb drives, flash drives, or jump drives). Please refer to the SHS Mobile Devices Security Guidelines policy for more information on this category of devices.
      vi. Compact Disk (CD) burners
      vii. Wireless routers or switches
   b. Connecting a personal wireless device to the SHS production wireless network, unless given specific approval from an SHS user authority.
   c. Installing or modifying components in any SHS-owned computing devices, unless for a specifically authorized business purpose, including, but not limited to:
      i. Random Access Memory (RAM) or hard drive storage
      ii. Wireless cards or adapters
      iii. Video cards
      iv. Compact Disc (CD) or Digital Video Disc (DVD) players or burners
   d. Installing software on computing devices operated within the SHS network. Software requests must first be approved by the requester's manager and then be made to the IS Department. Software must be selected from an approved software list, maintained by the IS Department, unless no selection on the list meets the requester's need. The IS Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.
   e. Attempting to circumvent or disable any SHS technical security control, including, but not limited to:
      i. User authentication mechanisms
      ii. User access privileges

iii. The web proxy, which controls which websites Workforce Members may visit.
iv. Anti-Virus software
v. Whole disk and data encryption
vi. Data Loss Prevention tools
vii. Activity Logging and Monitoring

f. Any activity that is illegal under local, state, federal or international law while utilizing SHS resources.
g. Creating, using, or distributing copies of SHS-licensed software that is not in compliance with the license agreements for the software.
h. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SHS.
i. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which or the end user does not have an active license.
j. Accessing SHS data, an SHS server, or an SHS account for any purpose other than conducting approved SHS business.
k. Introduction of malicious programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) into the SHS network or onto an SHS server or other asset.
l. Revealing an SHS account password to others, including family and other household members when working remotely.
m. Writing down or in any other manner capturing account user names and passwords and failing to secure that information. For example, it is not permissible for a workforce member to write his or her user name and password on a sticky note and affix the note to the computer monitor or place it anywhere around the workstation.
n. Using or allowing another individual to use an SHS account that has not been issued to them.
o. Using or allowing another individual to use an SHS-issued employee badge to gain access to the SHS network or any SHS information asset.
p. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
q. Making fraudulent offers of products, items, or services originating from any account.
r. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the workforce member is not expressly authorized to access, unless these duties are within the scope of regular duties.
s. Port scanning or security scanning unless that activity has been approved by the SHS IS Security Department.
t. Executing any form of network monitoring that will intercept data not intended for the workforce member's computer, unless that activity is a part of the workforce member's normal job/duty.
u. Interfering with or denying network or computing services to any workforce member unless specifically authorized.
v. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a workforce member's computer or network usage unless specifically authorized.

w. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material, to individuals who did not specifically request such material (email spam).
x. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
y. Revealing any confidential or proprietary information, trade secrets, or any other material covered by the SHS Confidential and Proprietary Information policy.

4. Personal Use of SHS Information Resources
   a. The overriding principle that governs personal use of these resources is that reasonable and incidental unofficial use of SHS information resources is authorized only so long all of the following are true:
      i. The use does not present a security risk to the organization.
      ii. The use occurs only on the workforce member's personal time.
      iii. SHS incurs no additional cost from that use, other than the minimal cost incurred from ordinary material and wear-and-tear.
      iv. The use does not interfere with official business.
   b. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
5. Role-based Access:
   a. Access to SHS information assets is role-based. User Authorities are responsible for:
      i. Requesting appropriate assignment, modification, and termination of access required or no longer required by their staff and other authorized data users
      ii. Conducting periodic entitlement reviews of their staff and other authorized data users.
   b. Principle of Least Privilege: Access privileges for Workforce Members are limited to the minimum level necessary to be able to perform and complete their assigned duties or functions.
   c. Principle of Separation of Duties: To prevent the appearance of, or opportunity to, commit a non-compliant, abusive or fraudulent act, no one person will be responsible for completing or controlling an entire business process from beginning to end
   d. Principle of Minimum Necessary: Access to SHS protected information is limited to only the information required to perform a particular job-related task or function, or to achieve an authorized requestor's specific purpose.
   e. Emergency Access: In the event of an emergency, SHS may provision access to individuals on a temporary basis based on the role that the individual are fulfilling during that emergency.
6. Information Security Awareness Training**:** All members of the SHS workforce are required to complete Information Security Awareness training at the time of hire and on an annual basis thereafter.
7. Workforce Separation or Transfer Events
   a. SHS departments, through accountable User Authorities, establish and maintain all necessary processes to disable workforce member's role-based privileges to all SHS information assets when a workforce member is terminated or transferred.
   b. Terminated or transferring Workforce Members may not retain, give away, destroy and/or remove from SHS any SHS information assets (electronic or hardcopy) and/or SHS information resources.
   c. All SHS information assets and information resources in the possession of the terminated workforce member must be turned over to the workforce member's manager prior to the time of departure. This includes, but is not limited to:

i. Computers
ii. Printers
iii. Software
iv. Cell Phones
v. Pagers
vi. Smart Phones
vii. Documentation
viii. Building Keys
ix. Encryption Keys
x. ID Cards
xi. Access Cards
xii. Electronic storage media, including CDs, DVDs, and USB storage devices

REFERENCES

- SHS Mobile Devices Security Guidelines
- SANS Institute Consensus Policy: Acceptable Use Policy
- 45 CFR Section 164.308(a)(3) (i) Workforce Security, (ii) (A) Authorization and/or Supervision, (B) Workforce Clearance Procedure, (C) Termination Procedures
- 45 CFR Section 164.308(a)(4) (i) Information Access Management, (ii) (B) Access Authorization, (ii) (C) Access Establishment and Modification
- 45 CFR Section 164.308(a)(5) Security Awareness and Training
- 45 CFR Section 164.312(a)(1) Access Control, (2) (i) Unique User Identification
- SHS Code of Conduct and Business Ethics
- SHS Social Media Policy
- SHS Corporate Integrity Program: Minimum Necessary Standard
- SHS Information Privacy and Security Investigation and Corrective Action policy
- SHS Employee Termination Checklist
- SHS Employee Transfer Checklist
- SHS Confidential and Proprietary Information policy
- SHS Non-Discrimination policy
- Website Exception Request Work Instruction

REVIEW/REVISION HISTORY

Date of Revision	Revision #	Revision / Review	Revision Description	Collaborated With (i.e. Standardization Committee, VP's, Quality, Risk)
10/27/2011	0	New		Compliance Committee
10/29/2012	1	Revision	Minor revisions	ISO
07/27/2015	2	Revision	Significant revision to update and make more comprehensive	ISO
7/27/2016	3	Revision	Addressed unauthorized software and user authentication using the employee badge	ISO
8/22/2016	3	Review		Policy and Benefits Committee

7/13/2017	4	Revision	Added section and additional content addressing Internet usage. Archived Workstation Use and Workstation Location policies.	SHS Privacy and Security Workgroup, Policy and Benefits Committee for information
11/14/17	5	Revision	Addressed Guest Internet	SHS Privacy and Security Workgroup, Policy and Benefits Committee for information
4/18/2018	6	Revision	Minor edits and revisions	SHS Privacy and Security Workgroup, Policy and Benefits Committee for review (8/2018)