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

Policy & Procedure

Page 1 of 6	Revision #: 4
Owner: Administration	Authorized by: Strategic ERM Committee

Confidential and Proprietary Information

APPLICATION

All SHS Workforce Members.

POLICY

1. All information concerning patients, physicians, employees, volunteers, financial data, and business records is confidential/proprietary. All employees and students of SHS will conform to this rule of confidentiality and information will not be disclosed unless authorized or required by law. Confidential and proprietary information will be destroyed in accordance with the SHS Record Retention and Destruction policy.

2. Discussions regarding confidential information shall take place in an appropriate setting to minimize disclosure to unauthorized individuals.

3. SHS Workforce Members, physicians, volunteers, and students are responsible for safeguarding patient and member information, or other sensitive business information, against loss, destruction, tampering, and unauthorized copying, access, or use.

4. Only authorized users will be allowed access to computer systems or networks. The security and integrity of computerized information are the responsibility of each system user.

5. Failure to adhere to policies on confidential information and protection of patient privacy may result in corrective action as referenced in the Information Privacy & Security Investigation & Corrective Action Policy.

PROCEDURE

DEFINITIONS:

A. **Break the Glass:** A warning or alert in an electronic medical record system that displays when an end user attempts to enter an individual's record, or information contained in the record, that is considered particularly sensitive or confidential. When an end user "Breaks the Glass," additional auditing and monitoring of access for appropriateness may occur. Typically, the end user must enter their system username and password and acknowledge a reason for entering the record to ensure access and use of the information is minimally necessary and for a legitimate purpose.

B. **Confidential Materials Lock Bin:** A locked container used to collect all paper recycling (confidential and non-confidential). Keys to these locked bins are maintained by Facilities staff, Environmental Services, and SHS Couriers responsible for taking the contents of these bins to an approved facility or vendor for shredding.

C. **Confidential Trash:** Any material that contains financial, administrative, and/or clinical results that can be associated with the name of a patient, employee, student, volunteer, or physician. Confidential Trash will be disposed of through established Confidential Trash systems within each department.

D. **Green Confidential Shred Bag:** A secure drawstring bag, usually green, that lines the Confidential Shred Bin and is used to collect and securely transport paper recycling for shredding.

E. **Proprietary Information and Materials**: Information and materials developed during employment and belonging to SHS, e.g., inventions, program and research development, marketing and selling, patentable developments, computer software, documents, case studies, course outlines, tape recordings, films, advertising materials, mailing lists, visual aids, and other materials.

F. **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:
   1) The individual's past, present or future physical or mental health or condition;
   2) The provision of health care to the individual; or
   3) 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).

G. **Sensitive Information**: Information, in any form or media, concerning SHS patients or members; workforce members including physicians, employees, volunteers, or students; financial data; or other proprietary or confidential information that should not be made public or shared without appropriate authorization or as required or authorized by law. Sensitive Information includes but is not limited to PHI, PII, personal credit card information, business records, employment records, SHS financial data, SHS or system/vendor proprietary information, etc.

IMPLEMENTATION:

1. Appropriate confidentiality statements will be signed by each employee or student at the time of hire or placement.
   A. All employees will sign a Code of Conduct Statement and an Employee Confidentiality Statement. These statements will be signed at the time of orientation and retained in the employee personnel files in Human Resources. Compliance will be assessed at the time of performance appraisals.
   B. Volunteers will sign Volunteer Confidentiality Statements when they begin volunteer work. These statements will be retained in the volunteer personnel files in the Volunteer Services office.

C. Clinical affiliation agreements with colleges and universities will include reference to student responsibilities regarding confidentiality of information and protection of patient privacy.

2. Appropriate hospital and department policies and procedures will be reviewed during orientation.
   A. New employees and students will review pertinent policies on management of information, confidentiality, and patient privacy as part of department orientation.
   B. Volunteers will receive instruction regarding patient rights and confidentiality.

3. Computer system and network access will be approved by the department manager and the Information Systems Department.

4. Termination of privileges: Upon termination of employment or transfer to another job classification, the following security issues will be addressed by the transferring/terminating manager:
   A. Notify Information Systems to delete access to hospital networks.
   B. Access/passwords to department computers/network will be removed.
   C. Department equipment/property in possession of employee will be returned.

5. Some Individual records, or specific information in the Individual's record, may be particularly sensitive or confidential. SHS may place these records or information behind Break the Glass in order to prevent incidental or unauthorized access or use of information, or to minimize inappropriate disclosure of the information. Break the Glass may be applied in the following situations:
   A. When additional auditing and monitoring for appropriate access and use of the information is necessary to minimize access due to curiosity or concern;
   B. When the information, if used or disclosed, could cause harm to the patient or others;
   C. When there is a legal hold on the record due to active or pending litigation;
   D. When other business needs necessitate monitoring or limiting access to an Individual's record.

   Break the Glass may be placed on a patient's record within the Epic application suite with approval from the SHS Privacy Officer, Health Information Management Director, or their designee. To request Break the Glass on a specific patient's record, contact the IS Service Desk at 541-768-4911.

   Other SHS systems may have differing abilities with respect to Break the Glass functionality. For assistance reviewing or placing Break the Glass on information in these systems, contact the IS Service Desk as well for review.

6. As appropriate a department may develop policies, procedures, and guidelines that address department-specific issues related to the types of information used in the department and access/restriction by information type and job responsibility. Department policies and procedures may include reference to the following:
   A. Patient information (medical records needed for patient care, medical information provided to other organizations for continuing care, insurance and/or billing information, data for research purposes).
   B. Physician information.
   C. Hospital information (hospital statistics, quality improvement data, state and federal reporting data, financial information).
   D. Physical security measures (times when departments, offices, or equipment should be locked, combination-locked doors, computer passwords, security software, alarms).

E. Computer systems and network access and back-up procedures. Procedures for recovery of critical information will be included in department disaster plans.

7. Wherever possible, Sensitive Information shall be discarded in a designated Confidential Materials Lock Bin. All paper recycling, regardless of how it is collected or whether it contains Sensitive Information or Confidential Trash, is submitted to an authorized firm or location where it is destroyed in accordance with NIST standards for confidential destruction.
   A. Paper waste that may or may not include PHI can be collected in general recycle bins in departments or areas that do not have enough space for a Confidential Materials Lock Bin. Workforce Members are responsible for ensuring the contents of these individual recycle bins are deposited into designated Confidential Materials Lock Bins (or directly into Green Confidential Shred Bags used to collect and transport Confidential Trash by Environmental Services, SHS Couriers, or other departments responsible for handling Confidential Trash). The contents of these bins are routinely collected and taken to an approved facility or vendor for shredding.
      1) To retrieve a document inadvertently deposited into a Confidential Materials Lock Bin, contact the SHS Couriers, Facilities, or other authorized person to unlock the bin and retrieve the necessary information. Retrieval of information should be observed by the Workforce Member's manager, supervisor, or other individual authorized to unlock the Confidential Lock Bin to ensure any information other than the intended document is returned to the Confidential Lock Bin and not inappropriately retained.
   B. Medical waste including blood viles, medications, urine cups, IV bags, or other items that may include a patient identifying label or PHI are also destroyed in a confidential manner. Patient labels must either be removed and placed in a Confidential Materials Lock Bin for shredding, or the waste processed and destroyed in such a way that the label is rendered unreadable or indecipherable.
   C. Electronic devices that may store PHI or other sensitive information (i.e.; USB devices, CDs, hard drives, etc.), should be sent to SHS Information Services for proper destruction.
   D. Refer to Appendix A for additional details.

REFERENCES

- 45 CFR 164.530(C)
- 45 CFR 164.310(d)(2)
- Data Storage Destruction Policy
- National Institute for Security and Technology (NIST) Special Publication 800-88: *Guidelines for Media Sanitization*

REVIEW/REVISION HISTORY

Date of Revision	Revision #	Revision / Review	Revision Description	Collaborated With (i.e. Standardization Committee, VP's, Quality, Risk)
Date Released	0	New		
12/10/2012	0-1	Revision	Archived	
12/10/2012	2	Revision	Added definition of proprietary information. Archive SAGH Confidential and Proprietary Policy	Legal/Compliance

7/20/2016		Review		
3/29/2018	3	Revision	Clarified policy on shredding of all recyclable materials, standardized definitions Minor GME revisions at P&B Committee 6/14/2018	Information Privacy and Security Committee, Professional Development, Graduate Medical Education
4/16/2019	4	Revision	Added additional language regarding disposal and handling of Confidential Trash and Break-The-Glass	Information Privacy and Security Committee, SHS Couriers, Facilities Management, Environmental Services, SHPO Compliance and Clinic Admin
		Select		
		Select		

Appendix A: Disposal and Destruction of Confidential Information

	Details	Handling
Paper	Confidential or non-confidential papers	Paper waste can be disposed of in individual recycle bins in a safe, secure location. Empty individual recycle bins on a regular basis into Confidential Lock Bins. Confidential Lock Bins are picked up and contents shredded by SHS Couriers and/or designated vendor. Never include the following items in Confidential Shred Bins: • Paperclips • Three-ring binders • Sharps • IV bags • Unused medications • Other medical waste
Electronic Devices	USBs, CDs, hard drives, etc.	Send the device to SHS Information Services or call 541-768-4911 for assistance
Non-Paper Materials	Biomedical waste, sharps, IV bags, specimen cups, etc.	Dispose of biomedical materials in identified bio-hazardous waste collection bins OR remove any patient labels or other identifiers prior to disposal. Deposit labels in bins designated for Confidential Shredding. Dispose of sharps in designated sharps collection bins.