PURPOSE: To supplement and support University of Kansas (KU) I.T. policies and to establish management direction, procedures and requirements for appropriate administrative and physical access control of Student Health Services (SHS) information systems, assets and communications areas, especially those involving electronic protected health information, or “ePHI”.

GENERAL PROVISIONS: Access to information resources, tools and workstations is solely granted for those purposes authorized by SHS Administration and to carry out SHS job duties. This is with the understanding that resources will be used in an ethical and lawful manner. All such access must be formally approved by SHS management. (Refer to AD-301 Authorization of Access to Information Systems)

POLICY: In order to protect the confidentiality, integrity and availability of all data received, created and maintained by SHS it is imperative for proper control measures to be followed. Proper compliance will ensure confidentiality, integrity and availability of ePHI as required for patient care, regulatory compliance and professional ethics. All workforce members are stakeholders and share a measure of responsibility in intrusion detection, prevention, and response. As such, all workforce members are to report any unauthorized access attempts or other improper usage of KU information systems.

- Attached is a grid (AD-302-A) showing the information systems used by SHS and their “criticality” to SHS operations. Storage of Electronic Protected Health Information is STRICTLY limited to the systems noted as being used for treatment (“T”) and for payment (“P”).
- In general, the presence of patients, visitors, family members, former employees and vendor representatives is to be controlled so that they do not have access to any workstation, electronic media, network device, wiring closet or other area in which protected health information is received, processed, stored, archived or transmitted.
- All SHS workforce members who have a job-related need to access protected health information are subject to University and SHS access authorization requirements.
- All workforce members are to wear an Identification badge or lab coat (with embroidered name) at all times when present within SHS.
- It is the responsibility of all SHS personnel to question (in an appropriate manner) the presence of any person in an area or anyone looking at information that
seems to be inconsistent with this policy. If concerns remain after questioning this person, he/she is to be asked to leave the area or SHS with the assistance of Administration or KU Office of Public Safety as appropriate.

- All non-patient visitors (vendor representatives, service technicians, etc.) are to present proper photo-identification to the supervisor of the department in which they are visiting.
- When possible, an accommodation will be provided to personnel from KU Computer Center and from Network Telecommunication Services (NTS) in the performance of their duties within SHS.

**PROCEDURE:**

1. Workforce Clearance, Access, Modification and Removal – Refer to AD-301 Authorization of Access to Information Systems

2. Workstation – Also, refer to AD-303 Workstation Use
   2.1. I.T. will maintain a log of equipment received and disposed and the method used to remove ePHI from the drives. If the device is intended for re-use, this too will be noted and tracked.
   2.2. I.T. will comply with the Computer Center’s procedure for “cleansing” hard drives and for disposing of equipment.


4. Portable / Mobile devices (laptops) Owned by SHS
   4.1. The user must sign a AD-302-1 Portable Device Receipt & Acknowledgement form which delineates the unique security issues arising from the use of portable devices.
   4.2. Laptops are configured with Computer Center-approved image.
   4.3. SHS will maintain a few laptops for temporary use. These are to be signed-out in a log maintained by the I.T. office.
   4.4. No ePHI may be stored on this device without prior approval of Administration. If approved for such use, I.T. is to be informed of this fact when the laptop is returned and I.T. will ensure it is properly removed.
   4.5. If laptop is assigned to a staff member on a semi-permanent basis, it is understood that the user may remove the device from SHS on an as-needed basis without a requirement that it be signed-out through I.T.
   4.6. By virtue of this device being used in lieu of a workstation, its antivirus code will be updated at regular intervals whenever the user logs in to the network.
   4.7. Whenever possible, any SHS information, files, etc. retained on the hard drive should be moved to a network drive for the same reason that desktop hard drives are not an appropriate place for storing such information.
4.8. If the mobile device is to be used in a semi-permanent location that is occasionally unattended and/or open and difficult to secure (such as Urgent Care), the device will be protected with an I.T.-approved anti-theft device.

4.9. Upon termination of employment or upon request from management, the employee is to return the laptop.

4.10. If the portable device is removed from SHS, the user must take steps to protect the device from:
- Loss or theft – For example: Do not leave in unattended vehicle, or in locations that make it easily viewable by others, etc.
- Unauthorized access – For example: Do not allow family or friends to use the device, etc.
- Extreme heat or cold
- Introduction of malicious code

5. Privately Owned Equipment

5.1. No privately-owned equipment may be attached to any SHS computer equipment or the KU network without Administrative approval. Examples of such would include:
- Telephone
- Printer
- PDA / Cell phone
- Thumb drive / Flash drive
- Laptop / Notebook computer
- External CD/DVD drive or other external hard drive

5.2. SHS intends to provide the workforce members with the necessary equipment to perform their jobs. If the person believes an exception should be made, the respective supervisor is to be the first point of contact. If the supervisor believes an exception is justified, Administration is to be consulted.

6. Printers

6.1. May be connected by way of the network or directly (“locally”) connected to the workstation

6.2. Used for printing work-related documents

6.3. Located in non-public areas so as to protect the privacy of printed documents. Printed output should not be allowed to stack-up to the degree that others without the “need-to-know” have access to the output.

6.4. Connection and assignment of printing locations is determined by management in concert with I.T. staff and is not to be changed except by I.T.

6.5. In addition to a departmental printer, SHS will attempt to provide each user with access to a high-volume printer/copier.

6.6. Each supervisor and each provider will have a personal printer at their respective desk. Non-supervisory staff will not be provided with personal printers unless specifically approved by Administration.

7. Document scanners:
7.1. The location assignments for document scanners will be tightly controlled and
determined by Administration in consultation with I.T. and supervisors.
7.2. The only locations to have these devices for scanning documents into the
electronic record within Point and Click will be R&R, Business Office, I.T. and
Laboratory.
7.3. All registration check-in locations as well as the Business Office and Pharmacy
will have insurance card scanners.
7.4. The Pharmacy will also have a scanner for scanning prescriptions into
ProPharm.

8. Facsimile “Fax” Machines:
8.1. May be used for sending and receiving work-related documents
8.2. Must be located in non-public areas so as to protect the privacy of original and
printed documents; originals and printed output should not be allowed to stack-
up to the degree that others without the “need-to-know” have access to the
documents.
8.3. Use of speed-dial buttons is encouraged, however, the fax numbers assigned to
the buttons are to be verified for accuracy on a periodic basis.
8.4. Must comply with any other policy established by SHS for faxing of information.

9. Removable or “External” Media – (Magnetic disks, compact disks, flash drives,
micro-drives, external hard drives, etc.)
9.1. Use is limited to those individuals with a demonstrated, work-related need; SHS
Administration must approve of such use.
9.2. May not be used for storage or archiving of ePHI.
9.3. May not be stored in any area to which the public has ready-access
9.4. Must be stored in protected locations
9.5. Personally-owned disks or devices are not to be used for SHS business unless
otherwise approved by I.T. It is the intent of SHS to provide all media and work
tools needed for SHS business.

10. Servers: Servers are located within the Computer Center and are under their
responsibility for physical access control, administrative control, backup, updating,
etc., while working in collaboration with I.T. staff (within SHS). Refer all questions
regarding physical access controls and protections for servers to Computer Center.

11. Software Owned by SHS:
11.1. The I.T. department is charged with the responsibility for logging, filing,
and safeguarding all software media and manuals (as appropriate) along with all
licenses.
11.2. This documentation extends to any “shareware” or “freeware” used by
SHS.
11.3. These logs will be made available for any KU audit of such assets.

12. Network Wiring Closets:
12.1. Doors are to be locked at all times.
12.2. Access is strictly limited to I.T., and staff from the Computer Center and NTS; these individuals must ensure physical security of the closet when work is finished.
12.3. Any changes or modifications to the network infrastructure must be documented by the involved party.
12.4. No food or drinks are to be in the wiring closets.


14. Security Incident Reporting – Any user that observes or learns of a security incident or abuse problem of a KU information resource is to immediately notify the I.T. department and/or SHS Administration. SHS will comply with KU’s Information Technology Security Policy and the following procedure:
14.1. Take immediate minimal steps as necessary and possible to ensure the security and integrity of information resources. This is necessary to protect KU resources from further incidents as well as to help secure forensic evidence.
14.2. Immediately notify the Director of SHS, or her designee. Documentation of this incident is to be done as soon as possible by way of completing a "Notice of Event" form (AD-101-1).
14.3. In addition, immediately contact the KU Help Center (864-0200), and follow any process as directed by the KU IT Security Office.
14.4. SHS Administration will work closely with the Office of the Vice Provost for Information Services and Office of Human Resources for disposition as necessary related to violation(s) of University policy.

15. Environmental service personnel are not permitted to read, access, move or remove PHI in any form. They are not to be in any area containing files of PHI (like R&R, B.O., etc.) without staff from that department being present throughout the cleaning process.

16. Other outside service technicians and company representatives are considered to be under the supervision of the respective department they are visiting here at SHS. The supervisor for that department is to validate the identity of the individual and ensure that he/she has no access to information, systems or areas except as necessary for the provision of service.

17. Personnel from KU’s Facilities Operations Dept. may access SHS for work-related needs. At no time are they to read, access, copy or remove PHI in any form or media.

18. Any maintenance activity to physical security features of the facility (e.g., exterior lighting, doors, locks, alarms, etc.) will be logged by the Supervisor of Purchasing.
19. No University-owned information system property, hardware or software may be removed from SHS without signing-out the item(s) from I.T. Depending upon the planned use, it may be necessary for the user to obtain approval from Administration.

GLOSSARY OF TERMS:

- **Information Security Incident**: Any action that has the potential to pose a serious risk to campus information system resources or the Internet. Includes but is not limited to:
  - Creating and propagating viruses and/or worms and other malicious code
  - Obtaining or allowing unauthorized access to University resources, including ePHI
  - Sharing ePHI without authorization
  - Deliberate attempts to deprive authorized personnel of access to any University computer system or network
  - Falsifying or otherwise corrupting of information and data
  - Sharing User IDs and passwords
  - Installing unapproved software/hardware
  - Unauthorized modification of system configuration or settings
  - Deliberate attempts to degrade the performance of a computer system or network or otherwise intentionally disrupting services or damaging equipment, software, files, or data

- **Malicious code**: A program or string of programming code that was designed to compromise data integrity and/or availability of information systems; examples: “virus,” “worm,” “Trojan horse,” etc.

- **Personal Digital Assistant (PDA)**: A handheld device that provides storage of calendars, and contacts at a minimum, with more advanced models being capable of wireless Internet access and email, photography and mobile phone service.

- **Protected Health Information (PHI)**: Health information that is individually identifiable health information and is transmitted or maintained in any form or medium, including electronic (ePHI), paper and oral.

- **Strong password**: As defined by KU policy, a strong password is one that prevents an unauthorized person from guessing or otherwise determining another person’s password. A Strong password is characterized by a combined use of letters (both upper and lower case), numbers and special characters. Please refer to KU policy on current requirements for a strong password.

- **Workforce members**: Employees, volunteers, trainees, students and other persons under the direct control of SHS, whether or not they are paid by SHS or KU.
REFERENCE:
This policy is intended to support and further clarify (for purposes within SHS) the University of Kansas I.T. policies found at:  http://www.policy.ku.edu/it/index

“Acceptable Use of Electronic Information Resources”
https://documents.ku.edu/policies/Information_Services/General_IS/Acceptable_Use/Acceptable%20Use.htm

Other related policies in SHS:
AD – 301 Authorization of Access to Information Systems
AD – 303 Workstation Use and Security