UNIVERSITY OF KANSAS
WATKINS HEALTH SERVICES
ADMINISTRATION

NUMBER:	ISSUE DATE:
AD-302	**2/15/2005**
TITLE: **Security Management of Protected Health Information (PHI)**	**REVISED:** **5/7/2019**
TITLE OF OWNER: **Director**	**APPROVED:** **Director**

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 Watkins Health Services (WHS) file locations, information systems, assets and communications areas, especially those involving PHI which may include electronic protected health information (ePHI).

GENERAL PROVISIONS: Access to information resources, tools and workstations is solely granted for those purposes authorized by WHS Administration and to carry out WHS 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 WHS management. (Refer to AD-301 Authorization of Access to Information Systems)

POLICY: In order to protect the confidentiality, integrity and availability of all information received, created and maintained by WHS it is imperative for proper control measures to be followed. Proper compliance will ensure confidentiality, integrity and availability of PHI and 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 record storage locations or KU information systems.

- Attached is a grid (AD-302-A) showing the information systems used by WHS and their “criticality” to WHS operations.
- In general, the presence of patients, visitors, family members, former employees and vendor representatives is to be controlled to the degree that they do not have access to any storage location, workstation, electronic media, network device, wiring closet or other area in which PHI and ePHI is received, processed, stored, archived or transmitted.
- All WHS workforce members who have a job-related need to access PHI and ePHI are subject to University and WHS access authorization requirements.
- All workforce members are to wear an Identification badge or lab coat (with embroidered name) at all times when present within WHS.
- It is the responsibility of all WHS 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 to leave WHS

with the assistance of Administration or KU Office of Public Safety as appropriate.

- All non-patient visitors (e.g. 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 in the performance of their duties within WHS. These people are to be wearing a Computer Center identification badge.

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. WHS Information Technology (I.T.) will maintain a log of equipment received and disposed of and the method used to remove ePHI from the hard drives / internal storage media. If the device is intended for re-use, this too will be noted and tracked.
   2.2. I.T. will comply with the KU Computer Center's procedure for decommissioning hard drives and other data-storage devices, and for disposing of equipment.

3. User ID and Passwords – Refer to AD-301 Authorization of Access to Information Systems

4. Mobile devices Owned by WHS
   4.1. The user must sign a form AD-302-1 Mobile Device Receipt & Acknowledgement which delineates the unique security issues arising from the use of mobile devices.
   4.2. Mobile devices are configured with Computer Center-approved image when available. WHS will comply with other KU-mandated features to safeguard these devices when possible, e.g. whole-disk encryption.
   4.3. WHS maintains laptop computers or tablets for temporary use by WHS personnel. 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 or mobile device is assigned to a staff member, it is understood that the user may remove the device from WHS on an as-needed basis without a requirement that it be signed-out through I.T. An example would be a device being used for presentations on campus or in the community or working from home. The exception to this is Nursing Staff members who are assigned a laptop to perform their duties in patient care. Nursing staff need permission from their supervisor to take the device offsite or home.

4.6. WHS laptops and workstations follow the KU IT policies of encrypted hard drives using Bitlocker AES-128. Bitlocker keys are managed by Safeguard which is a product of the Sophos antivirus suite KU IT uses to protect our equipment.
4.7. 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.
4.8. Whenever possible, any WHS 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.
4.9. 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 Treatment Clinic), the device will be protected with an I.T.-approved anti-theft device.
4.10. Upon termination of employment or upon request from management, the employee is to return the mobile device.
4.11. If the portable device is removed from WHS, 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 computer code, i.e. malware.

5. Privately Owned Equipment
5.1. No privately-owned equipment may be attached to any WHS computer equipment or the KU network for the purpose of conducting WHS work without Administrative approval. Examples of such would include:

- Telephone
- Printer
- Mobile phone
- Thumb drive / Flash drive
- Laptop / tablet computer
- External CD/DVD drive or other external hard drive

An exception is allowed when connecting mobile devices for battery re-charging.

5.2. WHS 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 connected to the workstation, i.e. a “local” printer.
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 remain on the printer output tray to enable others without the "need-to-know" to have access to the document.
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, WHS will attempt to provide each user with access to a high-volume printer/copier.
6.6. Each supervisor and each provider will have a local printer at their respective workstation. Other WHS 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. All registration check-in locations as well as the Business Office and Pharmacy will have insurance card scanners.
   7.3. The Pharmacy will also have a scanner for scanning written 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 remain on the fax machine to enable others without the "need-to-know" to 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 WHS 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; WHS 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 WHS business unless otherwise approved by I.T. It is the intent of WHS to provide all media and work tools needed for WHS business.

10. Servers: Servers are located within the KU Computer Center and are under their responsibility for physical access control, administrative control, backup, maintenance, etc., while working in collaboration with WHS I.T. staff.

11. Software Owned by WHS:

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 WHS.
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 controlled by staff from the KU Computer Center. 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.

13. Individuals representing entities outside of KU seeking access to the Network/Information systems – Refer to AD-301 Authorization of Access to Information Systems.

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 WHS Administration. WHS 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 WHS Administration. 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. WHS Administration will work closely with the proper KU authorities for investigation, mitigation and resolution 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 while in WHS. The supervisor or designee for that department is to validate the identity of the individual and ensure that person has no access to information, systems or areas except as necessary for the provision of service.

17. Personnel from KU's Facility Services Dept. may access WHS 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 related to physical security features of the facility (e.g., exterior lighting, doors, locks, alarms, etc.) will be logged by WHS Administration.

19. No University-owned information system property, hardware or software may be removed from WHS 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.
- 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, photographic and oral.
- Social Engineering: Psychological manipulation of people into performing actions or divulging confidential information, done for the purpose of information gathering, committing fraud or system access. Examples:
  - Baiting – A malware-infected device (e.g. USB drive) is left in a place where it will likely be found and used by someone.
  - Phishing – Sending a fraudulent email disguised as legitimate from a trusted source aimed at convincing the recipient to share personal information or to click on a link or attachment that installs malware.
  - Spear phishing – Phishing which is aimed at a specific person, e.g. a person in authority and/or likely to have access to sensitive information.

  - Scareware – A message that involves convincing a user into thinking the computer / network resources are infected with malware then offering a solution to fix the bogus problem which will actually infect the computer if downloaded.
- 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. 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 WHS, whether or not they are paid by WHS or KU.

REFERENCES:

This document is on file with the KU Policy Library.

KU I.T. Policy: "Acceptable Use of Electronic Information Resources"
http://policy.ku.edu/IT/AcceptableUse

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