**Security Standards for the Protection of Electronic Protected Health Information Used in Business Associate Related Projects**

**at the University of Kansas (Lawrence) [[1]](#footnote-1)**

**A. Introduction**

The Health Insurance Portability and Accountability Act (HIPAA) is the federal legislation that governs the uses and disclosures of protected health information (PHI) in order to protect individuals’ privacy. HIPAA’s ***Privacy Rule*** establishes the conditions under which health information, regardless of the form or medium of that information, maintained by *covered entities* and by *business associates* performing services on behalf of covered entities, may be used or disclosed. HIPAA’s ***Security Rule*** addresses the security of protected health information in electronic form only. This document addresses the Security Rule as it applies to KU-Lawrence investigators who are not themselves in covered health care components of the university, but who receive or collect electronic protected health information while acting as a **business associate** of the covered entity.[[2]](#footnote-2)

Note that the standards contained in this document apply only to electronic protected health information as defined in the HIPAA Security Rule. These standards would not apply, for instance, to protected health information that has been de-identified. Limited data sets must be safeguarded in accordance with the requirements of the applicable contract or data use agreement.

**B. Definitions**

**Covered entity.** A health plan, a health care clearinghouse, or a health care provider which electronically transmits any health information in electronic form. Generally, these transactions concern billing and payment for services or insurance coverage.

**Business associate.** An entity independent of a covered entity that performs certain functions or activities that involve the use or disclosure of protected health information for or on behalf of a covered entity.

**Individually identifiable health information.**  Information that is a subset of health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual, and that identifies the individual, or with respect to which there is a reasonable basis to believe that information can be used to identify the individual.

**Protected health information (PHI).** Individually identifiable health information held or maintained by a covered entity or its business associate that is transmitted or maintained in any form or medium, including electronic, paper, and oral. This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse.

**ePHI.** Protected health information in electronic form.

**Principal investigator (PI).** The person responsible for the research or service project which involves protected health information.

**Persons with access.** All persons authorized to have access to the electronic protected health information on the research or service project for which the Principal Investigator is responsible.

**C. Roles and Responsibilities**

1. The **Vice Chancellor for Research** is the institutional official responsible for the development and implementation of the policies and procedures related to protected health information received from a covered entity for research purposes or related to services performed for a covered entity as a business associate.
2. The **Human Research Protection Program (HRPP)** is the Institutional Review Board (IRB) which reviews proposed protocols for research involving human subjects to help ensure that there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of their data, regardless of the format of the data.
3. The **HIPAA Coordinator** provides training and expertise to Lawrence personnel working with PHI, helps formulate policy, and works to ensure that the university complies with the HIPAA regulations.
4. The **Coordinator of Information Technology and Planning** contributes to the development of policies relating to information technology on behalf of the Vice Provost for Information Services.
5. The **IT Security Office,** a division of Information Services, is responsible for coordinating information technology security at the university and for providing security-related support services. Information technology policies and procedures can be accessed on the web at <http://www.security.ku.edu> or by calling (785) 864-9003.
6. **Technical Liaisons.**  Security management at the university is largely decentralized. Where appropriate, certain responsibilities for information technology security have been delegated to Technical Liaisons working within the various university departments and units. Each department or unit is required to register a Technical Liaison with the IT Security Office.
7. **Departments/Units.** While Principal Investigators are ultimately responsible for the security of ePHI utilized within their projects, such ePHI often necessarily resides on equipment and systems maintained by their departments or units. In such cases, PIs and their respective departments/units must work together to ensure that the ePHI is maintained according to the requirements set forth in this document. Specifically,
	* 1. University departments and units with systems containing ePHI must comply with these requirements, university policies and procedures, and laws addressing the privacy and security of such information and address environmental or operational changes affecting the security of such information.
		2. Each university department or unit, in coordination with its Technical Liaison and with its PIs working on projects involving ePHI, must provide for periodic review and revision of its security policies and procedures to address technological, environmental, or operational changes.
		3. Each department or unit with systems containing ePHI must arrange for a periodic Risk and Vulnerability Assessment (RVA) by the IT Security Office. The RVA shall evaluate the potential risks and vulnerabilities to confidentiality, integrity, and availability of ePHI held by the department or unit, as well as identification of measures sufficient to reduce such risks and vulnerabilities to a reasonable and appropriate level. The RVA guidelines may be viewed <http://security.ku.edu>.
		4. Each department or unit with systems containing ePHI must establish an IT Contingency Plan in the event of an emergency such as fire, vandalism, system failure, or natural disasters for systems that contain ePHI. For assistance in devising a Contingency Plan, contact the IT Security Office (864-9003).
8. **Principal Investigators.** Principal Investigators are responsible for:
9. Drafting a project data security plan, typically in conjunction with the department or unit Technical Liaison, to ensure that PHI accessed or obtained during the course of a project is properly safeguarded. The project data security plan should be kept and maintained by the PI to document the safeguards taken to protect the confidential data. The plan should be reviewed annually by the PI and the Technical Liaison prior to applying for an HRPP project approval update. Access a [sample template for a project data security plan](http://research.cms-dev.ku.edu/human-subjects-research-forms).
10. Submitting a signed Risk Management Certification to the Human Research Protection Program (HRPP) as a prerequisite to receiving approval for the HRPP application from the Human Research Protection Program Lawrence Campus (see [Appendix V,](#AppendixV) *Project Risk Management Checklist and Certification*). The Risk Management Certification serves to affirm that a data security plan has been developed and that appropriate safeguards have been established.
11. Maintaining an inventory of the ePHI accessed, created, received, stored, and transmitted by the PI and persons with access and the hardware and electronic media containing the ePHI. The inventory should detail the location of the hardware and electronic media and the person responsible for them. The inventory must be updated as changes occur.
12. Maintaining the confidentiality, integrity, and availability of the ePHI.
13. Protecting against any reasonably anticipated threats or hazards to the security or integrity of such information.
14. Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law.
15. Compliance with these requirements, university policies and procedures, and laws addressing the privacy and security of such information. All requirements contained in a Business Associate Agreement with a Covered Entity or in a sponsored agreement with a Covered Entity must also be honored. To the extent that the requirements of such agreements are more stringent than these requirements, the more stringent requirements will apply.
16. Addressing environmental or operational changes affecting the security of such information.
17. Assuming responsibility or appointing an individual to be responsible for the on-site coordination of activities relating to compliance with these guidelines and with state and federal privacy laws.[[3]](#footnote-3)
18. Mitigating, to the extent practicable, any harmful effect that is known of a use or disclosure of PHI that is in violation of applicable policies and procedures or of state or federal law.
19. Documenting compliance with these guidelines. Documentation must be maintained for a minimum of six years following the end of the project.

**D. Reporting Breaches of ePHI**

The following procedures should be followed when any unauthorized disclosure or use of ePHI on a project is discovered or suspected:

1. Leave the equipment powered on and the network cable plugged in so that evidence is not destroyed. Do not further investigate or otherwise touch the affected computer/system/server.
2. Notify the Vice Provost for Research by calling the Research Compliance Help Line (864-7444) ***and*** notify the Information Technology Security Office by calling the KU Help Desk (864-0200). These offices will contact and work with the Human Research Protection Program, the HIPAA Coordinator, the KU Crisis Coordinator, the Public Safety Office, and the Office of the General Counsel to respond to the incident.
3. The computer/system/server cannot be put back into service until released by the IT Security Office.  Response to the incident may involve eliminating network access to the device

**E. Sanctions**

The unauthorized disclosure or use of ePHI is a violation of federal law as recorded in 45 CFR Parts 160 and 164 and offenders may be subject to the governmental penalties described therein. Depending on the nature of the violation and the employment and/or academic status of the individual, an offender may also be subject to sanctions contained in university policies regarding scientific and scholarly misconduct, student academic misconduct, information technology security, and employee misconduct.

**F. Information Access Management**

1. **Allowing Access to ePHI**
	* 1. **Authorization of Access to ePHI.** Principal Investigators are responsible for designating the personnel who need access to ePHI to perform the project. Authorization of access to systems containing ePHI must be documented (see [Appendix II](#AppendixII), Sample Authorization of Access to Information Systems). The PI must annually review the permitted authorizations for persons with access as part of the risk management check.
		2. **Minimum Necessary Access.** Access must be commensurate with the person’s role on the project. Access must be limited to the minimum level of PHI appropriate to the person’s role in the project.
		3. **Confidentiality and Security Agreements.**  Prior to being granted access to ePHI, individuals requiring access must sign a Confidentiality and Security Agreement (see [Appendix I](#AppendixI)). These agreements should be held by the Principal Investigator responsible for the project.
		4. **Subcontractors and Service Providers.** In cases where access to ePHI must be granted to a subcontractor or outside vendor, the agreement with the subcontractor or outside vendor must clearly contain the same standards for safeguarding the ePHI as are contained in this document. The covered entity’s requirements regarding the handling and use of ePHI, as stated in the sponsored agreement and/or business associate agreement, must also be clearly stated in the agreement with the subcontractor or service provider.
2. **Access Authentication.**
3. Each PI and/or department or unit must establish and implement procedures to verify the identity of the person or entity prior to granting access to the ePHI.
4. Persons seeking access to any network, system, or application must not misrepresent themselves by using another authentication device.
5. Persons with access are not permitted to allow other persons or entities to use their unique authentication device.
6. **Termination of Access.**  Principal Investigators must establish a process to terminate on a timely basis an individual’s access to ePHI upon completion of the project or when that individual’s role in the project has ended. The process must include a mechanism to document and confirm termination of the individual’s access to the ePHI (see [Appendix III,](#AppendixIII) *Sample Termination of Access Checklist*). Procedures relating to termination of access to ePHI must provide for:
7. Deactivation of relevant user accounts and removal from relevant access control lists.
8. Changing of codes for key punch systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information.
9. Changing the combinations of combination lock mechanisms.
10. Retrieving physical access control items, such as keys, ID badges, smart cards, and tokens.
11. Retrieving university-issued devices and storage media, such as portable computers, PDAs, pagers, cellular phones, DVDs, CD-ROMs, diskettes, and other electronic storage media.
12. Steps necessary to ensure that locked or encrypted files used by the departing person can be accessed by the PI. If proxy access is needed to applications or email used by the departing person, the PI should contact the System Access Office at 864-0439 upon receiving authorization from the Vice Provost for Research to be granted such proxy access.

If a PI has knowledge that a person with access poses a risk to the security of ePHI, the PI is obligated to take the necessary steps to remove that person’s access. Such steps should be taken in accordance with university policies such as the Code of Student Rights and Responsibilities, employment policies, and the Information Technology Security Policy.

**G. Facility Access Controls**

PIs and their departments/units are responsible for ensuring that the facilities, systems, and equipment used to store ePHI for their projects are safeguarded from unauthorized physical access, tampering, or theft. Such safeguards must include the following:

1. **Access Control and Validation.** Procedures must be established to control and validate an individual’s access to facilities housing ePHI based on the individual’s role or function. Examples include but are not limited to the following:
	1. Use of physical access control mechanisms, such as keys, code locks, or smart cards.
	2. Not allowing visitors access to any equipment or devices storing ePHI.
	3. Requiring persons with access to wear identification badges when on site.
2. **Maintenance Records.** PIs and their respective departments or units must manage and document repairs and modifications to the physical security components of the facility housing ePHI, such as locks, windows, doors, and other physical access control hardware.
3. **Contingency Operations**. PIs should establish backup and disaster recovery procedures in coordination with their department or unit’s Disaster Recovery/Contingency Plan.
4. **Privately-Owned Devices.** Privately-owned devices such as computers, PDAs, and external drives may be used to transmit, store, or transmit ePHI ***only if:***
	1. the use of the device(s) has been approved in advance by the PI; AND
	2. the device and its configuration have been approved in advance by the department/unit’s Technical Liaison.

Removal of ePHI from privately-owned devices must be verified by the PI or by the department or unit designate responsible for the security of ePHI as described in Section J.4.

**H. Workstation Use**

PIs and their departments/units must provide persons with access to workstations containing ePHI on their projects with the following information:

1. The proper functions to be performed on the specific workstation or class of workstations;
2. The manner in which such functions are to be performed on the specific workstation or class of workstations. For example:
	* 1. The required methods for securing the application when leaving the workstation unattended (logging out or “locking” the workstation, etc.);
		2. The manner in which storage media used with the workstation such as diskettes or CD-ROMs are to be securely stored;
		3. Prohibitions regarding the practice of writing down user IDs and passwords where others can find and or use them; and
		4. The process, where applicable, for making backups on a regular basis to protect against business interruption.
3. Requirements regarding the physical attributes of the surroundings of a specific workstation or class of workstation. For example:
	* 1. Prohibitions on leaving the workstations unattended for prolonged periods of time while active;
		2. Prohibitions on moving workstations without approval of the PI; and
		3. Securely locking the room in which the workstation is located; and
		4. Taking measures to minimize casual viewing by passersby, such as turning off the monitor or using a polarized screen filter.

**I. Password Management**

1. **Unique User IDs and Passwords.**  Persons with access to networks, systems, or applications used to create, transmit, receive, or store ePHI must be supplied with a unique user identification and password in order to gain access to the ePHI.
2. **Generic User ID and Passwords.** A generic user identification and password may be utilized for a shared or common area workstation so long as the login provides no access to ePHI. An additional unique user identification and password must be supplied to access applications and database systems containing ePHI.
3. **Password Security.** Practices regarding the use of passwords must comply with the university’s password policy ([www.policy.ku.edu](http://www.policy.ku.edu/)).

**J. Security of Servers, Workstations, Mobile Systems**

Servers, workstations, and mobile systems used to access, receive, store, or transmit ePHI must be maintained in accordance with the security standards that comply with university policies ([www.policy.ku.edu](http://www.policy.ku.edu)) and state and federal laws, regardless of whether these systems are overseen by a PI directly, by the PI’s department or unit, by Information Services, or by a third-party service provider. Before undertaking a project involving ePHI, the PI must determine who will assume responsibility for the security of the systems involved, and take reasonable steps to document that the responsible party understands and accepts those responsibilities. In the case of a third-party service provider, such steps must include incorporating language into the vendor agreement that explicitly states the security standards required.

1. **Security safeguards include, but are not limited to:**
2. ePHI must be housed:
	* 1. in the KU Computing Center, in the area designated by the IT Security Office for this purpose; **OR**
		2. in a physically secure, non-networked system; **OR**
		3. in a secure environment approved by the IT Security Office or by the Office of the Vice Provost for Research.
3. The system administrator or root account must be password protected.
4. A user identification and password authentication mechanism must be implemented to control user access to the system. Mobile devices such as laptops must use a boot password to ensure that the system is only accessible to authorized users.
5. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the potential severity of the vulnerability.
6. All unused or unnecessary services must be disabled.
7. Virus detection systems must be implemented including procedures to ensure that virus detection software is maintained and up to date.
8. Workstations and mobile devices located in unattended, common, or otherwise insecure areas must implement the following measures:
	* 1. A password protected screensaver or automatic logoff mechanism. The location of the device and the sensitivity of the ePHI must be considered when determining appropriate time out periods.
		2. The device’s screen or display must be situated in a manner that prohibits unauthorized viewing. Use of a screen guard or privacy screen is recommended.
		3. A theft deterrent device, such as a cable locking mechanism.
9. Mobile devices must be stored in a physically secure location when not in use.
10. **Firewall Use**

Networks containing ePHI-based systems and applications must implement perimeter security and access control with a firewall. Firewalls used to protect such networks must conform to standards established by the IT Security Office.

1. **Remote Access and Wireless Access**

The university’s Office of Information Services has developed policies and procedures for remote access and wireless access to university networks, systems and applications (see Virtual Private Network (VPN) Service on the University of Kansas Data Network and the Wireless Local Area Network (LAN) Systems Policy at www.policy.ku.edu). In order to provide for the security of ePHI, approval must be obtained from the IT Security Office (864-9003) prior to implementing wireless or remote access.

1. **Device and Media Controls and Disposal**

Either the PI or the department or unit responsible for the security of the ePHI must address the receipt and removal of hardware and electronic media such as hard drives, removable disks, floppy drives, and CD ROMs into and out of the secure areas as well as the movement of such items within the secure area (see [Appendix IV,](#AppendixIV) *Disposal or Return of Confidential Data*). Such procedures must:

1. Provide for a determination as to whether a retrievable copy of ePHI is required prior to movement, re-use, or disposal.
2. Address the final disposition of ePHI, and/or the hardware or media on which it is stored.
3. Address removal of ePHI from electronic media before it is made available for re-use.
4. Provide for a record of the movements of hardware and electronic media and the person responsible therefore.

Information regarding acceptable methods of data removal/destruction may usually be found in the terms and conditions of the sponsored agreement and/or the business associate agreement with the covered entity/sponsor. University standards for cleaning or sanitizing equipment and storage media are available at <http://www.security.ku.edu>.

* 1. **Encryption and Security**

Project data should be encrypted whenever possible, particularly when such data is transmitted electronically through email or file transfer, when being archived off-site, or when stored on a mobile device. Use of email to communicate PHI is strongly discouraged. PIs should consult with their department or unit’s Technical Liaison or the IT Security Office for additional information regarding the availability of technology to protect confidential data contained in standalone files, email communications, and data passed between a web browser and web server. Policies and procedures regarding the applicable requirements for, and limitations on, the transmission of ePHI must be clearly communicated to persons with access.

* 1. **Data Integrity**

Each PI or department/unit must develop and implement a plan to prevent or detect unauthorized alteration or deletion of ePHI or critical system and network files where deemed reasonable and appropriate based on the project security plan, for example:

* + - 1. Running automated integrity checks against files or file types containing ePHI or determined to be critical;
			2. Assigning responsibility for reviewing the results of integrity checking and handling discrepancies; and
			3. Restoring any ePHI that may become corrupted.

**K. Activity Control and Review**

Each PI or department/unit must develop and implement a plan for monitoring the system activity where deemed reasonable and appropriate based on the project’s data security plan. The extent, frequency, and nature of these reviews must be determined by the project’s security environment. The procedures for system activity control and review must:

1. Identify the systems and applications for which system activity will be monitored;
2. Identify the information to be logged for each system;
3. Establish the hardware, software and/or procedural mechanisms that will be used to record and examine activity, such as utilization of logs, access/activity reports or other mechanisms;
4. Provide for review of the system monitoring setup by an appropriate individual (such as the Technical Liaison) on a regular basis, at intervals commensurate with the associated risk of the information system and the sensitivity of the ePHI;
5. Provide for reporting of security incidents such as activity exceptions and unauthorized access attempts to the IT Security Office in accordance with the IT Security Policy. Breaches of ePHI should be reported as indicated in [Section D](#Breaches).

**L. Training Persons With Access**

Persons with access to ePHI must be provided with training regarding project-specific and department/unit-specific policies and procedures relating to the security of ePHI. Persons with access must also be provided with periodic updates on changes to university security policies and procedures as appropriate, including warnings regarding identified threats, breaches, vulnerabilities, or other security incidents. Assistance with such information is available from the IT Security Office, which has established a website at <http://www.security.ku.edu> with relevant resources. Training must be documented and updated as material changes in the IT security environment or procedures occur. Documentation may include a roster of attendance by persons with access and the curriculum for the training.

**M. Access to ePHI by Covered Entities**

This policy shall not be construed to prohibit access to ePHI by a covered entity which has provided the ePHI or on whose behalf the ePHI is being collected. Requests for access to ePHI by the covered entity should be directed to the PI of the project.

Appendix I

**Confidentiality and Security Agreement**

**Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Department/Unit\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Principal Investigator/Project Director\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. I recognize that I will have access to confidential data that is governed by University of Kansas policy and state and federal laws. Examples of confidential data include but are not limited to information pertaining to an individual’s physical or mental health and treatment, an individual’s financial information and other personally identifiable data, such as Social Security Numbers.

2. I recognize that data accessed by me may only be used to conduct the project as delineated by the project director in accordance with university and department or unit policies and procedures. I will not store, use, or access data except as permitted by the official policies and procedures of the university and my department or unit.

3. I recognize that disclosure of data is governed by the policies and procedures of the university and my department or unit, as well as by state and federal law. I will not release data in any circumstances other than those defined by the policies and procedures of the university or my department or unit; or as otherwise permitted or required by law and only after proper identification and verification of identity and authority is ensured.

4. I will not share sign-on passwords or log-on information with anyone except as requested by my supervisor or department/unit head, by an information services professional in order to resolve a technology problem, or by a university official or law enforcement official in an emergency situation (as permitted or required by applicable law) and only after proper identification and verification of identity and authority is ensured.

5. I agree to report loss of a password, or any actual or attempted unauthorized access, use or disclosure of confidential data to my supervisor or department/unit head and to other university personnel or officials as required by the policies or procedures of the university or my department/unit.

6. I understand that violation of these policies and procedures may result in disciplinary action, including but not limited to, privilege revocation and/or suspension or termination.

7. I understand that my obligations under this Agreement will continue after termination of my relationship with the university. Upon termination, I will immediately return any documents or media containing confidential data to the university.

8. I have read and understand this document.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_**

Signature Date

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_**

Principal Investigator/Project Director Signature Date

*The Principal Investigator/Project Director must maintain on file all Confidentiality and Security Agreements for the project.*

#### Appendix II

#### SAMPLE

#### AUTHORIZATION OF ACCESS TO INFORMATION SYSTEMS

User information

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

KU ID# (if a KU student): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This User is: \_\_\_ New

 \_\_\_Transferring from:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Current LAN administrator (if known):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| System | Role (Specify as Appropriate) | Comments |
| □ Network□ Remote Access |  |  |
| □ Email.\* |  |  |
| □ Internet |  |  |
| □ *[insert name of project/department/unit application(s)]* |  |  |
| □ Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |

\*Email—After the person with access’s paperwork has been processed through HR, please have her/him visit the following site to set up an Exchange email account if needed: <http://www.email.ku.edu/>. Notify the Technical Liaison when this is complete so that an Outlook profile can be set up on the machine.

\_\_\_\_ Please provide a User ID and temporary password(s) to access the above applications as part of this individual’s responsibilities.

I approve and request that the above named user be given the indicated level of access to the systems identified above.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Principal Investigator or Supervisor Name (Print)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Appendix III

#### Sample

#### TERMINATION OF ACCESS CHECK LIST

This checklist is intended as a guide for terminating a person’s access to University of Kansas facilities and information resources. If you believe that an individual’s access privileges should be suspended on an immediate basis to maintain the security, confidentiality and/or integrity of university data or IT systems, the Coordinator of IT Policy and Planning must be notified immediately at 864-4999.

## Employee Name/Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date:\_\_\_\_\_\_\_\_\_\_\_

**Department/Manager**:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1. University Property**

**\_**\_\_Returned desktop computers/laptops and accessories

\_\_\_Returned mobile phones and pagers

\_\_\_Returned other equipment/devices

\_\_\_Returned all computer disks, tapes, other electronic storage media

\_\_\_Returned other records, files

**2. Keys/Access Cards/Badge**

\_\_\_Returned all keys to facility/office/lab

\_\_\_Returned all keys to desk/filing cabinets/storage units

\_\_\_Returned all access cards

\_\_\_Combination locks changed

\_\_\_Returned ID Badge

**3. University Information Systems**

**\_\_\_**Provided location of all electronic information

**\_\_**\_Department/Unit Technical Liaison notified of change and the systems/applications accessed by exiting employee so that access can be terminated.\* (List systems/applications below)

 **1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **3.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **4.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **5.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Authorized Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date\_\_\_\_\_\_\_\_\_\_\_\_\_**

-------------------------------------------------------------------------------------------------------------------

**Confirmation of Access Termination:**

The above individual’s access to the systems/applications listed in section 3 has been terminated.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Technical Liaison or other Responsible Party Date**

Appendix IV

**Sample**

**DISPOSAL OR RETURN OF CONFIDENTIAL DATA**

|  |  |
| --- | --- |
| **Medium** | **Required Method**  |
| Computer Data–Computers & Hard Disk Drives |  |
| Computer Data–Stored on Server |  |
| Computer Data–Magnetic tapes |  |
| Computer Data–Floppy disks |  |
| Computer Data–Flash media |  |
| Computer Data–CD-ROM and DVD |  |
| Laser Disks |  |
| Microfilm/Microfiche |  |
| Paper Records |  |
| Videotapes |  |

If a project is externally sponsored, the required methods of disposal or return should correspond to any conditions specified in the grant or agreement document. Further information regarding appropriate removal or disposal of equipment or storage media housing confidential information may be found at <http://www.security.ku.edu>.

Appendix V

**Principal Investigator Project Risk Management**

**Checklist and Certification**

The certification form at the end of this Risk Management Checklist must be submitted to the Human Research Protection Program (HRPP) (C.8.b) for any project conducted under the terms of a business associate agreement with a covered entity under HIPAA. The Human Research Protection Program (HRPP) cannot approve an application to conduct such a project until it has received this signed certification that the required security standards are being addressed.

This internal checklist is intended to be a guide to the required standards regarding ePHI. For each security standard listed, identify the person on the project or within the department/unit responsible for ensuring that the requirement is being met. For example, projects relying primarily on their department/unit’s central computing resources might list the department/unit’s Technical Liaison as being responsible for specific IT security items. The checklist should be updated as personnel and their responsibilities regarding each requirement changes.

Requirements flagged with a “►” must be addressed prior to approval of the HRPP application by the Human Subjects Committee. The remaining requirements must be addressed as work involving ePHI commences. ***All requirements contained in this checklist are ongoing and must be maintained for the life of the project.***

|  |
| --- |
| **Administrative Requirements** |
| **Person Responsible** | **Requirement** |
| ► | The PI’s department/unit must schedule a periodic Risk and Vulnerability Assessment (RVA) by the IT Security Office (C.7.c) |
| ► | Prepare a project-specific Data Security Plan (to be reviewed annually by the department/unit’s Technical Liaison or other designated responsible individual) (C.8.a) |
|  ► |  An individual is assigned to be responsible for the on-site coordination of activities relating to compliance with these guidelines and with state and federal privacy laws (C.8.i) |
|  | Maintain an inventory of persons with access to ePHI (C.8.c) |
|  | Maintain an inventory of the ePHI accessed, created, received and stored for the project (C.8.c) |
|  | Document compliance with these guidelines (and maintain documentation for a minimum of six years following the completion of the project) (C.8.k) |

|  |
| --- |
| **Information Access Management** |
| **Person Responsible** | **Requirement** |
|  | Secure a *Confidentiality and Security Agreement* for each person being granted access to ePHI (F.1.c.) |
|  | Hold subcontractors or outside vendors to the same security standards as are contained in the KU policy (F.1.d.) |
|  | Document each authorization of access to systems containing ePHI (*Authorization of Access Form*) (F.2.) |
| ► | Procedures are established to verify the identity of a person prior to granting access (F.3) |
| ► | Procedures are established for terminating an individual’s access to ePHI (*Termination of Access Checklist*) (F.4) |

|  |
| --- |
| **Facility Access Controls** |
| **Person Responsible** | **Requirement** |
| ► | Procedures are established to control access to facilities housing ePHI (G.1.) |
| ► | A maintenance record of facilities housing ePHI has been created and will be kept up to date (G.2) |
| ► | Procedures are established to support restoration of data following an emergency in coordination with the department/unit’s Disaster Recovery/Contingency Plan (G.3) |
|  | Obtain the approval of the PI and the Technical Liaison prior to allowing ePHI to be housed on any privately-owned devices (G.4) |

|  |
| --- |
| **Workstation Use** |
| **Person Responsible** | **Requirement** |
|  | Persons with access to ePHI will be informed of the proper functions to be performed at their workstations (H.1) |
|  | Persons with access to ePHI will be provided with instruction regarding appropriate practices regarding workstation use (H.2 and H.3) |

|  |
| --- |
| **Password Management** |
| **Person Responsible** | **Requirement** |
|  | Each person with access to ePHI must be supplied with a unique user identification and password and must comply with the KU password policy (I.) |

|  |
| --- |
| **Security of Servers, Workstations, Mobile Systems** |
| **Person Responsible** | **Requirement** |
| **Security Safeguards** |
| ► | ePHI is located:* in the KU Computing Center; or
* in a physically secure, non-networked system, or
* in a secure environment approved by the IT Security Office or the Vice Provost for Research (J.1.a)
 |
| ► | System administrator accounts or root accounts are password protected (J.1.a) |
| ► | User identification and password authentication mechanisms have been implemented to control user access (J.1.c) |
| ► | Security patch and update procedures are established (J.1.d) |
| ► | Unused or unnecessary services are disabled (J.1.e) |
| ► | Virus detection systems have been installed and will be maintained (J.1.f) |
| ► | Workstations and mobile devices located in insecure areas: * have password protected screensaver or automatic logoff mechanisms installed
* are physically situated to prevent unauthorized viewing
* have a theft deterrent device installed (J.1.g)
 |
| ► | Mobile devices are stored in a physically secure location when not in use (J.1.h) |
| **Firewalls** |
| ► | Networks containing ePHI have a firewall in place (J.2) |
| ► | Firewalls have been configured in conformance with IT Security Office standards (J.2) |
| **Remote Access and Wireless Access** |
| ► | Approval from the IT Security Office has been obtained prior to implementing wireless or remote access to ePHI (J.3) |
| **Device and Media Controls and Disposal** |
| ► | Procedures are established for the disposal or return of ePHI (see *Disposal or Return of Confidential Data* form) (J.4) |
| **Transmission Security** |
|  | ePHI will be encrypted when transmitted over electronic networks unless an adequate alternative control has been identified and approved by the PI or department/unit (J.5) |
|  | Policies and procedures regarding the transmission of ePHI will be communicated to all persons with access (J.5) |
| **Data Integrity** |
| ► | A plan is in place to prevent or detect unauthorized alteration or deletion of ePHI and critical system and network files (J.6) |

|  |
| --- |
| **Activity Control and Review** |
| **Person Responsible** | **Requirement** |
| ► | The systems and applications which will be monitored have been identified(K.1) |
| ► | The information to be logged for each system has been identified (K.2) |
| ► | The mechanisms that will be used to monitor the activity have been established (K.3) |
| ► | Procedures for a regular review of the system activity are established (K.4) |
| ► | Procedures for reporting of security incidents are established (K.5) |

|  |
| --- |
| **Training Persons With Access** |
| **Person Responsible** | **Requirement** |
|  | Persons with access to ePHI will be provided with training regarding project-specific and department/unit-specific policies and procedures relating to the security of ePHI (L) |
|  | Training will be documented and training materials kept up to date (l) |

|  |
| --- |
| **Project Risk Management Certification****for KU-Lawrence Projects Conducted** **as a Business Associate of a Covered Entity** |
| Project Director/PI |  | Date Prepared: |  |
| Department/Unit |  |
| Project Title |  |
| Sponsoring Agency |  |
| HRPP # (s) |  | KUCR/KU Project # (if applicable) |  |
| Brief description of ePHI being accessed or collected and its intended use |  |

By signing this form, the Project Director/Principal Investigator of the above project agrees to maintain the security of electronic protected health information as prescribed by the university’s policies regarding security standards for electronic protected health information (ePHI) and by the requirements specified in the Project Risk Management Plan and Checklist for the life of the project.

HRPP Principal Investigator:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name (printed) Signature Date

Project Principal Investigator/Project Director (if different from HRPP Principal Investigator):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­­­­\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name (printed) Signature Date

Submit this certification page to HRPP. You may send your certification by email attachment, FAX (864-5049) or surface mail addressed to: HRPP, The University of Kansas, Youngberg Hall, 2385 Irving Hill Road, Lawrence, KS 66045. Questions may be directed to (785) 864-7429.

1. The information contained in this document shall be reviewed, evaluated and updated on a periodic basis by the Vice Chancellor for Research, the IT Security Officer, the HIPAA Coordinator, the Human Research Protection Program Lawrence Campus, and the Coordinator of Information Technology Policy and Planning. [↑](#footnote-ref-1)
2. Researchers working for one of the university’s clinics should refer to the university policy regarding the security of electronic health information for university clinics rather than this document. [↑](#footnote-ref-2)
3. An individual within a department or unit may be assigned such responsibility for many or all of that department or unit’s projects involving ePHI. [↑](#footnote-ref-3)