

HIPAA Policy on Research using Electronic Protected Health Information

University of Kansas Medical Center

April 2005

Policy

As required by the HIPAA Security Rule, the University of Kansas Medical Center (KUMC) provides administrative, physical and technical safeguards for electronic protected health information (ePHI) that is used for research. Responsibility for compliance with the Security Rule rests jointly with Principal Investigators (PIs), the HIPAA Compliance Program and the KUMC Department of Information Resources (IR). The Security Rule is found at 45 CFR, Parts 160, 162 and 164.

Background

The HIPAA Security Rule requires KUMC to assure the confidentiality, integrity and availability of ePHI. KUMC must protect ePHI that is created, received, stored and/or transmitted during research projects. HIPAA standards also apply after project completion, when computers, devices and/or media are destroyed or re-formatted for other uses. The HIPAA Compliance Program is responsible for educating the KUMC workforce about HIPAA standards.

The KUMC IR Department established policies and procedures to incorporate HIPAA Security Rule standards for administrative, physical and technical safeguards. The IR Department designs, develops, manages and assures the security of KUMC's technology infrastructure. The IR Department continually monitors network activity in order to detect and eliminate threats to data security.

The IR Department also creates and maintains both comprehensive security policies and HIPAA-specific policies recommended by the HIPAA Compliance Program. All members of the KUMC workforce must comply with the general security standards and responsibilities described in the KUMC Security Program Plan and other security policies posted at <http://www2.kumc.edu/ir/policy/>.

The policy statements below address specific requirements for researchers whose projects involve ePHI.

Definitions

Electronic protected health information (ePHI) means protected health information that is created, received, maintained or transmitted in electronic format. Protected health information is health data that is associated with one or more of the individual identifiers listed in Appendix A.

Administrative safeguards are administrative actions and policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect ePHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Physical safeguards are physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Technical safeguards are the technology and the policies and procedures for its use that protect ePHI and control access to it.

Confidentiality means the assurance that ePHI data is shared only among authorized persons or organizations.

Availability means the assurance that systems responsible for delivering, storing and processing ePHI are accessible when needed, by those who need them under both routine and emergency circumstances.

Integrity means the assurance that ePHI is not changed or destroyed in an unauthorized manner. It is an assurance that the information is authentic and complete, and that the information can be relied upon to be accurate for its purpose.

Principal Investigator is the individual with overall responsibility for the conduct of the study.

Procedures

Creation, Use and/or Receipt of ePHI

PIs are responsible for assuring appropriate oversight of research projects involving ePHI.

1. Creation, use and/or receipt of ePHI for research purposes requires prior approval by the KUMC Human Subjects Committee (HSC).
2. Collaborative research projects involving ePHI from another institution under approval by another institutional review board also must be submitted to the KUMC HSC.
3. Special procedures have been established to facilitate IRB review of joint projects that involve both the KUMC and KU-Lawrence campuses.
4. When receipt of ePHI will be covered by a business associate agreement or data use agreement, HIPAA Compliance personnel must review the agreement to ensure regulatory compliance.

Access of ePHI

PIs are responsible for ensuring that ePHI is accessed and used only by authorized research personnel for approved research activities.

1. Each individual involved in the creation, use or disclosure of ePHI must be named in the approved study personnel list on file with the HSC.
2. The PI is responsible for administering role-based access through appropriate account management. PIs should contact IR Customer Service to authorize access for approved study personnel.
3. The PI is responsible for assuring password protections on data files and for limiting password distribution only to authorized individuals.

4. PIs must notify Customer Service to terminate access when authorized personnel change status (e.g., change responsibilities, graduate, terminate employment) or when the project is complete. The PI must retrieve physical access control items such as keys, badges, smart cards and tokens when access is terminated or at project completion.

Storage of ePHI

PIs are responsible for secure storage of ePHI related to research.

1. Stored ePHI data should contain only the individual identifiers that are minimally necessary to support the research purpose.
2. As standard practice, research ePHI should be stored on KUMC network drives, such as (G: drive, K: drive or Q: drive). Storage on network drives maximizes data protection and ensures that KUMC meets HIPAA standards for authentication, intrusion detection, patch management, virus protection, disaster recovery and facility access control.
3. Mobile devices (laptops or PDAs) or electronic storage media (data sticks, tapes, disks, CD ROMs) may be used for temporary storage of ePHI if they are encrypted. Acceptable methods include hardware-based encryption or software provided or approved by Information Resources.
4. In addition to encryption, the PI is responsible for providing the following protections when ePHI is temporarily stored on devices or media:
 - a. Boot passwords and automatic logoff features;
 - b. Physical security of the device or media to prevent unauthorized access, tampering, loss or theft;
 - c. Current patch management and virus protection software;
 - d. Uploads to a secure network drive as soon as feasible, with a temporary storage time not to exceed 30 days;
 - e. Appropriate disposal, re-imaging or wiping of devices and/or media if they are re-used for other purposes.
5. If a study protocol requires long-term data storage on a stand-alone PC or sponsor-supplied laptop, those systems should be approved by the Information Security Office to ensure adequate security features, patch management and anti-virus protection.

Transmission of ePHI

PIs are responsible for assuring secure transmission of ePHI.

1. Electronic PHI that is transmitted to or from the KUMC network must be encrypted. Options include a dedicated transmission line, virtual private network, encrypted Web site and secure file transfer protocol (secure FTP).
2. Email communications between the Kansas City and Wichita campuses remain behind a network firewall and therefore meet security standards; further encryption is not required. Email communications between the KUMC and KU-Lawrence campuses require encryption when ePHI is being transmitted.
3. When electronic storage media are used for data exchange, the media must be password protected. Passwords must be sent to the data recipient in a separate secure communication.

Disposal of ePHI

PIs are responsible for meeting federal, legal and institutional requirements for disposal of ePHI.

1. Equipment and storage media must be sanitized prior to disposal or re-use. PIs should coordinate disposal and/or re-use through the KUMC Safety Office, in order to meet HIPAA standards.
2. PIs are responsible for following any additional requirements for study grants or contracts.
3. Disposal of research ePHI may not occur before minimum time frames outlined in the KUMC Research Records Retention Policy.

Reporting and Sanctions

PIs are responsible for reporting breaches of computer security related to ePHI.

1. PIs should inform the HSC if a breach of confidentiality occurs. The HSC will coordinate review by HIPAA compliance personnel. Technical sources of the breach will be addressed by the IR Security Office.
2. Sanctions against workforce members who violate the HIPAA Security Rule will be enforced in accordance with existing KUMC policies on disciplinary action.

Applicability

This policy applies to all users of ePHI belonging to KUMC and to related entities that use university networking services. Users include faculty, staff, postdoctoral fellows, students, residents and trainees.

Exemptions

None

Related Documents

HIPAA Security Rule (45 CFR Parts 160, 162 and 164)

KUMC HIPAA Security Rule Policy

KUMC Security Program Plan

KUMC Information Resources Policies

Contacts

KUMC Privacy Official
588-0942

KUMC Security Officer
588-0966

Appendix A
Protected Health Information (PHI)

If any of the following demographic characteristics are paired with information about past, present, or future physical or mental health, or information about the payment of health care, the resulting information is Protected Health Information under federal law.

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
 - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code