

HIPAA Security Rule Policy
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 that ensure the confidentiality, integrity, and availability of electronic protected health information under its control. Compliance with the HIPAA Security Rule is ensured by the collaborative efforts of the KUMC Department of Information Resources and the HIPAA Compliance Program.

Background

HIPAA Security Rule

KUMC is a covered entity under the HIPAA Security Rule. The Security Rule specifies administrative, physical and technical safeguards for electronic protected health information (ePHI). As a covered entity, KUMC must: (1) ensure the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted by the HIPAA Privacy Rule; and (4) ensure compliance with the Security Rule by its workforce.

Identification and locations of ePHI

Electronic PHI is created, received, maintained and/or transmitted by KUMC in support of the treatment, payment, operations, education and research functions. The university network protects ePHI under the control of KUMC and other campus entities: KU Physicians, Inc., KU HealthPartners, Inc. and the University of Kansas Medical Center Research Institute, Inc. Electronic PHI is located in formats such as: medical records applications, billing applications, file servers, email servers, stand-alone servers and workstations, medical equipment, mobile devices, storage media and databases used for clinical, education, and research purposes.

Definitions

Electronic protected health information means protected health information that is created, received, maintained, or transmitted in electronic format.

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 policy and procedures for its use that protect electronic protected health information and control access to it.

Procedures

1. The Information Resources (IR) Department designs, develops, manages, and ensures the security of KUMC's technology infrastructure. The IR Department designates a Security Officer who provides technical, policy and project leadership for all institutional electronic resources.
2. The IR Department creates and maintains both comprehensive security policies and issue-specific policies. KUMC workforce members are responsible for knowing and complying with all security policies. A list of relevant policies is found in Appendix A.
3. The university protects all electronic resources to ensure confidentiality, availability, and integrity. Electronic protected health information constitutes a subset of those resources that are protected. Electronic PHI is protected by administrative, physical, and technical safeguards that reflect best security practices.
4. Electronic PHI that is transmitted outside the KUMC network must be encrypted. Options include a dedicated transmission line, virtual private network, secure web server and secure file transfer protocol.
5. The university and its related entities practice role-based access to ePHI. Department administrators are responsible for determining appropriate access. Access is administered by IR Customer Services and/or administrators for individual resources.
6. Workforce training for compliance with the HIPAA Security Rule is incorporated into the Computer Security Awareness Training offered by IR. All users of university network resources complete security awareness training annually. The online training module includes information about best security practices and about Security Rule requirements. HIPAA Compliance personnel are responsible for monitoring and updating the training content related to the Security Rule. New employees must complete awareness training within 45 days of their start date. Training is delivered to new students and residents during orientation sessions. In addition to annual training, the Security Office issues updates and reminders as needed to disseminate new information or warnings about new threats.
7. The HIPAA Compliance Program conducts the comprehensive risk assessment that is required by the Security Rule. Findings and recommendations are reported to the Chief Information Officer and the Security Officer. The risk assessment is updated every two years.

8. The HIPAA Compliance Program ensures that university security policies and procedures meet the requirements of the HIPAA Security Rule for administrative, physical and technical safeguards. The HIPAA Compliance Program maintains and updates an inventory of safeguards that address Security Rule requirements.
9. The HIPAA Compliance Program identifies Business Associates who are involved in creating, receiving, maintaining or transmitting ePHI on behalf of the university. Program personnel ensure that Business Associate contracts reflect requirements of the Security Rule.
10. HIPAA personnel monitor ongoing and emerging issues related to the Security Rule. They consult with the Security Officer and other IR staff to implement changes as needed.
11. All KUMC workforce members are required to report suspected or known violations of the Security Rule. Reports should be made to the employee's supervisor or to HIPAA Compliance Program personnel. KUMC is required to enforce sanctions and mitigate damages to the extent possible.
12. Sanctions against workforce members who violate the Security Rule will be enforced in accordance with existing KUMC policies on disciplinary action.

Applicability

This policy applies to all users of electronic protected health information belonging to the University of Kansas Medical Center and to related entities who 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 Information Resources Policies and Procedures (Appendix A)

Contacts

KUMC Privacy Official
588-0942

KUMC Security Officer
588-0966

Appendix A
KUMC Policies that Support Compliance with the HIPAA Security Rule

Administrative Systems Backup Plan [Secured document]

Appropriate Use Policy
<http://www2.kumc.edu/ir/operationalprotocols/generaluse.asp>

Computer Security Policy
<http://www2.kumc.edu/ir/policy/security.asp>

Desktop Computer Standards
http://www2.kumc.edu/ir/operationalprotocols/pc_standards.asp

Disaster Recovery Plan [Secured document]

Electronic Equipment Disposal Policy
<http://www2.kumc.edu/safety/policies/pcdisposal.htm>

Incident Response Plan [Secured document]

Internet Use Policy
<http://www2.kumc.edu/ir/operationalprotocols/internetuse.asp>

Patch Management Plan [Secured document]

Password Security Policy
<http://www2.kumc.edu/ir/operationalprotocols/password.asp>

Perimeter Security Policy
<http://www2.kumc.edu/ir/operationalprotocols/perimetersecurity.asp>

Security Program Plan
<http://www2.kumc.edu/security/SecurityProgram-Public.html>

Virus Response Plan
<http://www2.kumc.edu/help/virusplan.asp>