KENTUCKY REGIONAL EXTENSION CENTER

HIPAA SECURITY RISK ANALYSIS

PROTECT YOUR DATA

All provider organizations, regardless of their size, are required to safeguard the confidentiality, integrity and availability of protected health information in any form.

Security breaches can leave you—as a provider or practice administrator—personally liable, facing monetary fines and jail time if you knowingly fail to protect this data.

Yet, we understand that limited staff and IT budgets often impose constraints in meeting these requirements.

Kentucky REC has an economical solution for you!

Our AHIMA certified specialists will conduct a risk analysis to evaluate your organization's compliance with the HIPAA Security Rule standards and implementation specifications. Our security professionals come with a wide range of technology backgrounds and industry certifications.

AUDITS

The HITECH Act requires periodic audits, performed by the Office for Civil Rights (OCR), to ensure covered entities and business associates are meeting HIPAA compliance requirements. Audits concentrate on adherence to three rules: HIPAA Privacy Rule, Security Rule, and Breach Notification Rule.

HIPAA Compliance/Enforcement *(AS OF 05/15)*

- Audit fines could result in $50,000 per violation and up to $1.5 million per violation of an identical provision in a single calendar year.
- 1 in 3 HIPAA complaints were investigated by the Office of Civil Rights (OCR).
- 1 in 5 breaches were due to unauthorized access and theft or loss of encrypted devices.
- 29.3 million patient health records have been compromised in HIPAA data breaches since 2009.

QUICK CHECK

- ☐ Who has access to your server room?
- ☐ Is your annual HIPAA training documented?
- ☐ Do you have a mobile device inventory; a disaster recovery plan; the required policies?
- ☐ How are employees granted system access?
- ☐ Do you have the latest wireless encryption?
- ☐ Have you performed a Security Risk Analysis?

SERVICE FEATURES

1. **HIPAA Security Rule Gap Analysis:** Review your current policies and procedures and identify compliance with the HIPAA Security Rule.
    - Provide guidance to organizations on how to comply with both the required and addressable HIPAA Security Rule standards.
    - Interview staff, officers, vendors and other key stakeholders as needed to gather necessary information.
2. **Facility Walkthrough Assessment:** Evaluate physical security.
3. **System Characterization:** Identify which assets store, transmit, or process e-PHI and create an inventory of those assets.
4. **Threat Identification:** Work with key stakeholders to evaluate the threats to the organization.
5. **Vulnerability Identification:** Work with key stakeholders to identify the absence, or weakness of, controls.
6. **Control Analysis:** Identify what controls are and are not in place.

Ask us about our new HIPAA Project Management Program!

7. **Likelihood Determination:** Evaluate the probability that a threat will exploit a vulnerability.
8. **Impact Analysis:** Evaluate the impact of an exploited vulnerability to the organization.
9. **Risk Determination:** Quantify the risk so that each identified risk can be prioritized.
10. **Control Recommendations:** Provide reasonable mitigation strategies for identified threats/vulnerabilities.
11. **Results Documentation:** Practice will receive a deliverable that outlines the entire process that was completed along with all findings and mitigation.
    - We will also provide policy and procedure templates that the organization can modify to use as their own.

KENTUCKY REC

Kentucky Regional Extension Center
2355 Huguenard Drive, Suite 100
Lexington, KY 40503

Toll Free: 888-KY-REC-EHR
Phone: 859-323-3090
Fax: 859-257-9366
Email: kyrec@uky.edu
http://kentuckyREC.com

UK UNIVERSITY OF KENTUCKY