



Legal Nurse Consultants: Backbone to the World of Risk Management

Volume 3 2016

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) instituted central national guidelines for security of protected health information (PHI). The Health Information Technology for Economic and Clinical Health Act (HITECH) instituted breach notification guidelines to provide transparency for those whose data may be at risk. HITECH requires the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to audit covered entities and business associates for compliance with HIPAA Privacy, Security, and Breach Notification Rules. In 2011 and 2012, OCR did pilot programs assessing processes of 115 covered entities to comply with HIPAA. OCR then assessed effectiveness of the programs.

Using evaluation results, in continued effort to assess compliance, OCR announced phase 2 has started, which will audit covered entities and business associates. OCR is creating improved sets of instructions to be used in audits and engaging a new approach to examine the efficacy of evaluating compliance efforts of the HIPAA regulated industry. The OCR states, "Audits are an important compliance tool for OCR that supplements OCR's other enforcement tools, such as complaint investigations and compliance reviews." Auditing covered entities allows OCR to "proactively uncover and address risks and vulnerabilities to protected health information."

The 2016 Phase 2 HIPAA Audit Program will appraise procedures implemented by covered entities and their business associates to meet standards of the Privacy, Security, and Breach Notification Rules. This is a significant part of OCR's overall health information privacy, security, and breach notification compliance activities. OCR employs the audit program to measure the HIPAA compliance efforts of entities. The audits present chances to scrutinize processes, identify best practices, and determine weaknesses that may not have surfaced during current compliance reviews. This empowers entities to confront problems before they result in breaches. OCR will generally identify best practices collected through the audit process and provide direction aimed at identified compliance challenges. LNCs can assist with audit preparedness.

Krug Consulting
was founded by
Sandra Krug,
RRT, CRNA
Legal Nurse Consultant.

AREAS OF PRACTICE:
Nursing Malpractice,
Personal Injury,
Product Liability,
Toxic Tort and
Environment,
Worker's Compensation
and Workplace Injury,
Criminal
Negligence,
Health, Illness or
Injury-related
Legal action,
Risk Management,
Nursing Home Abuse,
Fraud and Abuse
Compliance and
HIPAA,
Elder Law

info@LNCKRUG.com

5910 Post Blvd #110296,
Bradenton, FL
34211

1 (844) LNC-KRUG

LNCKRUG.com

Legal Nurse Consultants (LNCs) can play a vital role working with HIPAA covered entities, through their Risk Management programs. LNCs assist with conducting required risk analysis to determine any areas where there may be a need for new policies. This involves comprehensive and in-depth assessment of possible weaknesses to the confidentiality of electronic PHI. This should be the first step taken to ensure compliance. LNCs will alert these entities to the areas that may need immediate attention.

Administrative Precautions:

- Contingency plans to retrieve and restore any lost data in the event of an emergency: data backup, disaster recovery, emergency mode operation
- Incident reporting to identify and respond to any suspected or known security incidents
- Review information systems: audit logs, activity, access reports and incident tracking
- Risk management to implement policies to ensuring compliance with the Security Rule
- Sanction policies for employees who fail to comply with security measures
- Security avoiding unauthorized access to electronic PHI, including employee training

Physical Precautions:

- Disposal of electronic PHI addressed with policies, procedures and staff training
- Media re-use policy to address electronic PHI removed from media before return or re-use (copiers or scanners returned to leasing company, recycle laptops, etc.)
- Paper records shredded to render them indecipherable *Paper PHI may NOT be recycled

Technical Precautions:

- Emergency policies to obtain electronic PHI during power failure, natural disaster, etc.
- Unique User Id to allow entity to track use activity and prevent unauthorized access

Contact Krug Consulting to be matched with a nurse to assist your Risk Management team.