CTSI
Serving Colorado's Counties

Technical Update

Volume 15, Number 13 June 24, 2011

Auditing Your Protected Health Information (PHI) Systems

At this time, most PHI audits are being done on commercial entities and health clearing houses, which may include state systems. However, any privacy audit by the Office of Civil Rights can lead them to PHI records which could drag local governments into a larger privacy audit.

What This Means For Counties

To avoid this, take the following precautionary steps in any self-audit:

Find out if your records are in compliance with state and federal security standards for creating, storing, using, retaining and destroying protected health records regardless of source or location.

Make sure your policies give those persons who have rights in the PHI the notices and complaint procedures to which they are entitled.

Conduct periodic (every 2 or 3 years) risk assessments for all PHI retention systems regardless of size, location or purpose. Make inquiries regarding the knowledge and training of custodial employees part of that assessment.

Appoint a Privacy Officer to audit and oversee systems with the assistance of knowledgeable team members. Include someone on the team with the technical expertise to evaluate, locate, compare and purchase any necessary software encryption methods.

Document and retain in your management records all evidence of efforts to audit and improve compliance methods.

Implement any recommended security measures that the assessment team finds necessary to be in compliance.

Identify Privacy officers throughout the organization and keep a record of their group meetings and the training and information sharing they do to enhance their knowledge, task skills, and overall compliance efforts.

Make sure each unit has identified, in a poster or other policy, where PHI concerns are to be reported in writing and which staff person is responsible for the Privacy investigation records for each report.

For more information, contact CTSI at 303-861-0507.