CTSI
Serving Colorado's Counties

Technical Update

Volume 21 Number 39 August 22, 2017

The Cost of HIPAA Violations

In 2016, there were 12 monetary settlements for violations of Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. Each settlement averaged nearly $2 million. This made 2016 the biggest year for such payouts; however, 2017 is on track to beat that record with three more payouts in the first few months of the year in addition to an outright penalty $3.2 million.

HIPAA was signed into law in 1996 with the primary goals of insuring continuous health insurance coverage to people who lost or changed jobs, as well as lowering costs by standardizing rules for storing and transmitting protected health information (PHI). Part of the act deals with the safety and security of PHI. The Office for Civil Rights (OCR), part of the U.S. Department of Health & Human Services, offers training for health care organizations on the civil rights, health information privacy, and patient confidentiality laws that they are subject to under HIPAA. The OCR also audits organizations for compliance with HIPAA laws and investigates complaints concerning possible violations.

A Recent Case

The theft of a single laptop, containing electronic protected health information (e-PHI) for 2,462 patients, led to a recent HIPAA penalty of $3.2 million for the Children's Medical Center of Dallas. The laptop was stored in a secured area; however, the area was not restricted to only those employees allowed to access the e-PHI nor was the information on the laptop encrypted.

Children's had been previously warned about this practice by the OCR as early as 2007 and again after the loss of a Blackberry containing 3,800 patient records in 2010. Because of the prior warnings, Children's was fined $1,000 per patient record lost and $1,000 per day from September 30, 2010 to April 9,2013 for failing to encrypt the data as required by HIPAA's Access Controls standards after the previous incident. Additional fines were also levied resulting in the $3,217,000 penalty, which the hospital paid in full.

HIPAA penalties can add up quickly. The $1,000 per violation fine the OCR levied against Children's Medical Center of Dallas was actually the minimum allowable penalty under the law for a violation found to be "due to reasonable cause and not willful neglect."

What This Means for Counties

Penalties like these can be ruinous to small and mid-size health organizations, so it is important that you verify that you and any business with whom you might share PHI are in compliance with HIPAA guidelines. More information on HIPAA guidelines can be found at www.hss.gov/hipaa. You may also contact CTSI at 303-861-0507 with your questions. CTSI

800 Grant St., Suite 400
Denver CO 80203

County Technical Services, Inc.

303.861.0507
FAX: 303.861.2832