CTSI
Serving Colorado's Counties

Technical Update

Volume 13, Number 31 October 28, 2009

The HIPAA 2009 Interim Final Rule Concerning "Breach Notifications"- Part 1

On August 24, 2009, the Department of Health and Human Services issued an "Interim Final Rule" concerning "Breach Notifications" for Unsecured Protected Health Information under HIPAA. This rule became effective on September 24, 2009 and any breach occurring on or after October 24, 2009 is reportable. The purpose of this memo is to outline the major changes which may affect county units. The provisions apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information.

The definitions of "covered entity," "business associate," and "protected health information" used in the HIPAA Administrative Simplification regulations 45 CFR parts 160,162, and 164 at 160.103 have not changed. A "covered transaction" is also defined in the act. "Business Associate" means a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of individually identifiable health information. This includes but is not limited to persons who perform legal, actuarial, accounting, management or administrative services for covered entities and business associates, with limited exceptions.

"Unsecured protected health information" is protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance and provides that the guidance specify the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals (by definition of the Secretary of HHS). Protected health information under HIPAA generally does not include employee records; but under the Colorado Open Records Act, these employee records are afforded privacy.

The regulations define "data in motion" as that data moving through a network or wireless transmission and "data at rest" is data that resides in databases, file systems, flash drives, memory and any other structured storage method.

The Act requires covered entities to provide notice of breach securities to affected individuals and, for breaches involving more than 500 individuals, to the media, within 60 days of knowledge of the breach. A breach is the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of the information. There are two exceptions: (1) disclosures where the recipient of the information would not reasonably have been able to retain the information, or (2) certain unintentional acquisition, access or use of information by employees or persons acting under the authority of a covered entity or business associate, as well as (3) certain inadvertent disclosures among persons similarly authorized to access the PHI as a business associate or covered entity.

For further changes and what this means for counties, see "The HIPAA 2009 Interim Final Rule Concerning "Breach Notifications" Part 2" Technical Update.

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