

The HIPAA 2009 Interim Final Rule Concerning “Breach Notifications”- Part 2

The regulation states that “this guidance does nothing to modify a covered entity’s responsibilities with respect to the Security Rule nor does it impose any new requirements upon covered entities to encrypt all protected health information. The Security Rule requires covered entities to safeguard electronic PHI and permits covered entities to use any security measures that allow them to reasonably and appropriately follow all safeguard requirements. In addition to prosecution and penalties imposed by the department of HHS, portions of the rule will be implemented and enforced by the Federal Trade Commission. These are not expected to impact counties. However, it is expected that recipients of Medicare and Medicaid funds may be impacted.

A covered entity may avoid these Notice Requirements only if the data that is protected is secured by the specified means mandated by the Secretary of HHS. Those means currently require using a specified encryption system or a specified encryption algorithm. [Through the use of a mathematical algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form. Simpler forms of encryption may be decoded, but are generally the best means available to protect data.]

Total destruction of paper documents is also acceptable, but simple redaction of personal identifiers is not acceptable (45 CFR 164.514(e)(2) or 164.514(b)). Redaction may or may not result in the document containing information that no longer fits the definition of PHI and therefore a loss of that data may or may not be reportable. The rules caution

that “redaction is not a standardized methodology with proven capabilities to destroy or render the underlying information unusable, unreadable, or indecipherable”. Check the standards put out by NIST at www.csrc.nist.gov/ or www.csrc.nist.gov/ if your unit needs to understand the requirements of a group you work with.

What This Means For Counties

- 1) Assign a team of experts to review the regulations and re-evaluate the county’s health privacy practices to ensure compliance with all aspects of record protection. Even if HIPAA does not apply, the county may have many covered entities with whom they do business or they may need to beef up compliance with state privacy rules.
- 2) Check with Legal Counsel to see if additional language needs to be put into the Business Associate agreements that covered entities may have with the county, or that county entities may have with covered entities, especially regarding the storage, transmission, etc. of PHI on behalf of those covered entities.
- 3) Make sure that employees assigned custody of health records understand when, and when not to, transmit or provide health information to requestors. This should be the policy regardless of the source of the data, as once it is in the county’s hands it may not always be accompanied by the appropriately signed authorization forms, the signed business associate agreement, or the like.

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