HITECH

Health Information Technology for Economic and Clinical Health Act

---

WHAT IS HITECH?

Effective September 23, 2009, Health and Human Services (HSS) implemented the Health Information Technology for Economic and Clinical Health (HITECH) Act requiring covered entities under the Health Insurance Portability and Accountability Act (HIPAA) and their Business Associates to provide notification in the case of unsecured Protected Health Information (PHI) breach.

Guidelines specifying the methods that render PHI unusable, unreadable or indecipherable for relief from the breach notification requirement are also in the Act.

WHY DOES HITECH MATTER?

Fines for not complying with HITECH are expected to significantly increase over time. State Attorney Generals, the Federal Trade Commission, and Health and Human Services all have mandates to prosecute with increased scrutiny. Putting PHI in the hands of shredding providers does not absolve covered entities from paying for costly and timely breach notifications. Covered entities are not absolved until PHI is physically destroyed.

WHAT DOES HITECH REQUIRE?

A covered entity must notify each individual whose unsecured PHI has been believed to have been accessed, acquired, used or disclosed as a result of a breach. Should a breach involve more than 500 residents of a state, the covered entity must notify HSS and the media. Business Associates (third-party administrators or service providers) requiring access to unsecure PHI are also required to notify covered entities of breaches that occur while in their possession.

Additionally, the Act stipulates that encryption of electronic PHI and destruction of physical paper PHI are the only methodologies allowed in order for covered entities to be relieved of the breach notification requirement.

*PRO*SHRED®: A PARTNER IN COMPLIANCE

With ISO 9001 certified processes and over 30 years experience, covered entities trust *PRO*SHRED® to be an unparalleled extension of their organization to meet the HITECH Act requirements. We end breach notification fears by destroying all PHI on-site at the client location, with the highest level of security.