

Healthcare Information Technologies, LLC

HITECH Act: Privacy & Penalties

The HITECH Act brings with it expanded privacy and security laws that could significantly affect any practice. Changes have already been set in motion to begin this year (2010) with some beginning later. The application of these new regulations are rigorous and merit a full a understanding.

Who is involved? HIPAA now includes, in addition to practice personnel, everyone who is involved with the records. This covers business associates, vendors of EMR, technical staff, health information exchanges and staff at the hosting site if ASP or SAS.

What does it entail? Practices must track (have a comprehensive audit trail) ALL disclosures for the purposes of treatment, payment and health care operations. Patient has the ability to request disclosures for up to three years and practice must be able to facilitate this request in electronic form. Some systems often house admin and clinical data separately (the silo effect) in which case the practice will need multiple audit trails. Practice must also have a complete audit trail of who has accessed the patient's records internally.

Patients may restrict disclosures to health plans (for purposes other than treatment) if the patient has paid in full, out of pocket. Disclosures are now required to be the minimum data necessary to carry out administrative transactions. Practices must use de-identified patient data.

You are required to maintain a log of privacy breaches that affect fewer than 500 people and report this information annually to HHS. For breaches that affect 500 or more people, HHS and relevant prominent media outlets must be notified immediately as well. Each patient must be notified within 60 days of discovery of a breach by first-class mail or e-mail if that is the patient's preference with: 1) date and circumstances of the breach, 2) date of discovery, 3) type of PHI involved, 4) steps the person should take to protect himself or herself and to mitigate future damages, and 4) how the person can obtain more information about the breach.

Penalties Tier 1 Violation where the person did not (and by exercising reasonable diligence would not have known) that they violated the provision.

Penalties: \$100 for each violation to a maximum of \$25,000/year.

Tier 2 Violation that was due to reasonable cause and not to willful neglect.

Penalties: \$1,000 for each violation to a maximum of \$100,000/year.

Tier 3 Violation due to willful neglect and the issue is corrected.

Penalties: \$10,000 for each violation to a maximum of \$250,000/year.

Tier 4 Violation due to willful neglect and the issue is not corrected.

Penalties: \$50,000 for each violation to a maximum of \$1,500,000/year.

For example, if a physician or business associate does not properly notify patients of multiple breaches of confidential information, a penalty of \$50,000 for each failure to notify a patient may be imposed on the physician or business associate until the total reaches \$1,500,000. If the physician or business associate, in that same year, regularly discloses to third parties in a way that violates the regulations, the government can impose a penalty of \$50,000 for each improper disclosure until that total reaches \$1,500,000. The physician or business associate in that calendar year would then be required to pay \$3,000,000

Enforcement In addition to Federal Enforcement, the state Attorneys General are now empowered to Enforce and Fine. It is anticipated that this will become a revenue source for each individual state. Beware, Florida has heavily used this tactic in the financial sector for years.

To assure that as many violations as possible are detected, there is now a "whistle blower" provision which encourages insiders to report any perceived violation. They will be compensated by a percentage of the fines collected – this amount will be finalized by summer of 2012.