

**ALERT**  
**HITECH Act 2009 Changes to HIPAA**  
September, 2011

The American Reinvestment and Recovery Act of 2009 set aside twenty billion dollars to help healthcare organizations move toward the implementation of electronic medical records. Changes introduced in the Act directly affect all health care organizations, other entities which manage Protected Health Information (PHI), and vendors who may come in contact with PHI.

With this investment, HIPAA (the Health Information Portability and Accountability Act of 1996) was updated to enhance the privacy of the growing body of electronic medical records. This act's provisions went into effect February 17, 2010.

These changes, referred to as the HITECH Act (Health Information Technology for Economic and Clinical Health Act), expand HIPAA to cover a larger number of organizations by also applying to vendors who work with HIPAA Regulated organization (Covered Entities).

**Expanded Scope**

The Business Associates (IT Asset Disposition providers like Cascade) of Covered Entities are now held directly liable to the government in the same way as the Covered Entity, in terms of Security and Privacy requirements set forth by HIPAA. Business Associates are subject to the same civil and criminal penalties as the Covered Entities. Previous interpretations and enforcement were handled through service contracts between the Covered Entity and the Business Associate and Business Associates were held liable to the Covered Entity.

In order to comply with new HIPAA requirements, any Covered Entity that sends computer equipment, electronic media, or documents that potentially include PHI **must execute** a Business Associate Agreement ("BAA") with its IT asset (or document) disposition provider.

The Business Associate is required to implement certain controls, processes and trainings to comply with these regulations.

**Changes imposed by the HITECH Act:**

1. Covered Entities **must enter into contracts** with Business Associates and must publish who their Business Associates are.
  - This isn't a change from HIPAA, however more organizations will need to comply with the Privacy Rule as a result of the change in scope.
  - Contracts must exist and provide safeguards to conform to the HIPAA Privacy Rule.
  - All Covered Entities working with an IT Asset Disposition provider must enter into a Business Associates contract with them since it is likely the Business Associate will handle electronic devices containing PHI. The US Department of Health & Human Services has established a contract template for this purpose available at: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/contractprov.html>

2. Business Associates must comply with specific breach notification standards set forth by the Office of Civil Rights under Health and Human Services. This is the first federally mandated breach notification law.
3. Business Associates must appoint a Security Officer as well as conduct training, audits and have documented policies governing how electronic information from Covered Entities is handled to safeguard information in accordance with the Privacy Rule.
  - A guidance and explanation of suggested compliance methods is published at: <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>
4. The life cycle of electronic medical records is now considered more explicitly and data “In Disposal” is regulated as well by requiring methods of destruction which render data “unrecoverable” and “indecipherable”.
  - Although the HIPAA standards are technology neutral, the guidance offered is to follow the destruction standards recommended in the NIST 800-88 Guidelines for Media Sanitization. [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)
  - The Department of Health and Human Services put together a list of disposal FAQ’s: <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaq.pdf>
  - It is important for Covered Entities to audit or review the processes of their Business Associates to ensure conformance to HIPAA security requirements.

Along with the changes mentioned above are changes to the penalties. Business Associates can now be directly liable for breaches of PHI. The penalty for willful neglect has now been raised to \$1.5 million. Enforcement is promised to be improved and funding for the enforcement is paid for from the pool of penalties. The changes to the law are one of the reasons Cascade increased its Errors & Omissions coverage to \$5 million.

#### **Additional References:**

- Neil Peters-Michaud, Cascade CEO, 608-316-6637 or [nmichaud@cascade-assets.com](mailto:nmichaud@cascade-assets.com).
- Cascade’s Data Security overview: <http://www.cascade-assets.com/datasecurity.html>
- American Recovery and Reinvestment Act of 2009, Title XIII, (One Hundred Eleventh Congress, 2009)  
[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111\\_cong\\_bills&docid=f:h11enr.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h11enr.pdf)
- Summary of the HIPAA Privacy Rule, (U.S. Department of Health & Human Services, 2006)  
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>