The HIPAA Omnibus Rule as amended by HITECH was published in the Federal Register on Jan. 25, 2013, and became effective March 26, 2013. Covered entities and business associates were required to be in compliance with the new rule by Sept. 23, 2013. The final regulations recognize that renegotiating and amending existing Business Associate Agreements (BAAs) for HITECH compliance may be a burdensome task and included a one-year transition rule for entities that had existing BAAs in effect as of Jan. 25, 2013. That one-year transition period began Sept. 23, 2013, and expires Sept. 22, 2014.

Changes to the Business Associate section under HITECH include:

- Business associates (BAs) are now required to follow the same HIPAA rules as covered entities (CEs). Therefore, BAs must comply with the technical, administrative and physical safeguard requirements, as well as the policies and procedures and documentation requirements, for electronic protected health information (PHI) under the HIPAA Security Rule.

- The definition of a BA is expanded to include vendors that maintain, but do not view, patient information. The following types of vendors were added to the list of BA types: health information organizations, e-prescribing gateways or other persons who provide data transmission services of PHI to a CE and that require routine access to PHI. Also vendors who offer a personal health record (PHR) on behalf of a CE.

- A person becomes a BA by definition, not by the act of contracting with a CE or otherwise. Therefore, liability for impermissible uses and disclosures attaches immediately when a person creates, receives, maintains or transmits PHI on behalf of a CE or BA and otherwise meets the definition of a BA.

- Subcontractors of a BA are also liable for protections of patient information. BAs are required to have BAAs with their subcontractors.

- With the change in definition and responsibilities, BAs and subcontractors are now liable for civil and criminal penalties for violations of the Privacy Rule and Security Rule.

CONTINUED, NEXT PAGE
**Timeframe for BAAs**

The timeframe for updating BAAs are based on when the contract with the BA is updated. The transition rule gives the CE and BA, including subcontractors, operating under BAAs that were in place prior to Jan. 25, 2013, (including evergreen agreements) until Sept. 22 to amend their BAAs to comply with the HITECH requirements. However, this relief is only available if the existing BAA was not renewed or modified from March 26, 2013, to Sept. 23, 2013. If a BAA was renewed or modified during this period, the HITECH requirements should have been added at that time. Notably, this transition rule does not extend the time period for compliance with the underlying HITECH requirements; rather, it is a limited extension for renegotiating and amending BAAs.

**Steps to ensure compliance:**

- Make sure the BAAs in use have been updated. A sample agreement can be found on the HHS.gov website: [https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html)

- Review all vendor contracts to determine if the vendor meets the definition of a BA. Visit the AFMC HealthIT website to download a copy of the HIPAA/HITECH Business Associate Decision Tree: [https://afmc.org/healthit/toolkit/](https://afmc.org/healthit/toolkit/)

- Make a list of all BAs and review the current BAA in place. If it is not the updated version of the agreement, work to get new, compliant agreements signed with vendors.

**For more information**