

HIPAA UPDATE

The Health Information and Technology for Economic and Clinical Health Act (HITECH), which is Title XIII of the American Recovery and Reinvestment Act, was enacted by Congress on February 17, 2009.

HITECH increases your responsibilities regarding the requirements of Health Insurance Portability and Accountability Act (HIPAA) privacy and security provisions that are currently in place. As a courtesy, the following questions and answers were formulated to assist you in navigating HITECH and the HIPAA-related amendments.

Q: Does HITECH Act apply to me as a fully-insured group health policyholder?

A: No. If you are a fully-insured group health policyholder, HIPAA/HITECH does not apply to you. However, if you are self-funded group health policyholder and you qualify as a covered entity, HIPAA/HITECH does apply to you. We recommend you contact your legal advisor.

Q. Does HITECH Act apply to me as a business associate?

A. Yes. If you are a Business Associate under HIPAA, you are required to implement certain privacy as well as physical, technical and administrative safeguards, as required by HIPAA privacy and security regulations. The effective date for compliance is February 17, 2010.

Q. How do I know if I am a Business Associate?

A. If you receive, transmit, create, or maintain protected health information (PHI) or if you signed a business associate agreement with us, you are likely considered a business associate for purposes of HIPAA. Examples of a business associates include, but are not limited to, third-party administrators, sales agents/brokers, and vendors who have access to protected health information.

Q. If I signed a Business Associate agreement with a covered entity, is that enough?

A. You signed a Business Associate agreement with a covered entity, which made you contractually obligated to comply with certain aspects of HIPAA as outlined in your Agreement. HITECH now legally obligates you as a Business Associate to comply with certain HIPAA privacy provisions, HIPAA Security Rule and HITECH provisions.

Q. Are there other provisions of HITECH that a Business Associates must follow?

A. For the most part, a Business Associate must comply with all provisions of the HITECH Act. Therefore, we suggest you read it carefully. For example, a Business Associate must comply with the security breach notification provisions. If you experience a security breach as defined in HITECH, you must notify us in a timely manner and work with us to give notice to the affected individuals.

Q. HITECH mandates that Business Associates comply with a broad range of requirements found in the HIPAA Privacy and Security Rules. What types of measures should I have in place?

A. A Business Associates should have privacy and security policies that address:

- administrative, physical and technical safeguards;
- privacy and security training programs;
- confidentiality and/or nondisclosure agreements;
- reporting of privacy and/or security breaches;

- return/destruction of information upon termination of the BAA;
- process for providing an accounting of disclosures when requested or required;
- limit the use, disclosure and request of PHI to the minimum necessary;
- prohibit the sale of PHI in exchange for remuneration without an individual's authorization.

Q. What happens if I do not comply with the new legal requirements?

A. Under HITECH the fines have increased and are based on a new, tiered approach. The fine can range from \$100 per violation to \$50,000 per violation with a maximum fine amount of \$1.5 million for willful misconduct. Additionally, HITECH gives the State Attorneys General the ability to enforce HIPAA violations with injunctions and civil damages.

Q. What do I need to do if I am aware of an incident or breach?

A. When a Business Associate discovers a security breach of unsecured PHI, it must notify the appropriate Covered Entity immediately upon discovery of the breach. This new breach notification requirement does not replace existing breach notification state laws. Business Associates must comply with both the new federal requirements as well as applicable state law requirements.

Q. What types of incidents are considered a HIPAA security incident or breach?

A. Any unauthorized acquisition, access, use or disclosure of 'unsecured' PHI that compromises the security or privacy of the PHI.

Q. What happens if I do not comply with these security breach requirements?

A. If you experience a security breach and you have not implemented the HIPAA privacy and security rules, you may be fined by the Department of Health and Human Services.

Q. I have a small office. How can I comply with all the privacy and security requirements?

A. Compliance with the HIPAA Security Rule is scalable in approach. Even though as a Business Associate you must comply, your overall compliance approach depends on your (or your entity's)

- size, complexity, and capabilities
- technical infrastructure, hardware, and software security capabilities
- cost of security measures, etc.

Q. What if I have more questions about the HITECH Act, where else can I look?

A. We recommend that you contact an attorney or seek legal advice about your legal responsibility under HITECH because every situation is different. Also, you can reference many resources on the Internet, such as www.cms.hhs.gov.

Definitions

Business Associate:	Business Associate is a person or entity that performs a function, activity or service on behalf of a covered entity.
Covered Entity:	A covered entity includes certain health care providers, health plans and health care clearinghouses.
HIPAA:	Health Insurance Portability & Accountability Act
HITECH:	The Health Information and Technology for Economic and Clinical Health Act (HITECH), which is Title XIII of the American Recovery and Reinvestment Act, was enacted by Congress on February 17, 2009, which includes a provision amending the HIPAA privacy and security rules.

Protected Health Information (PHI):

Protected health information includes any individually identifiable information, written or oral, that is created or received by Covered Entities and Business Associates that relates to the individual's past, present, or future physical or mental health or condition or payment.

Assurant Employee Benefits is the brand name for prepaid dental products provided by one or more of the following legal entities: Union Security Insurance Company, DentiCare of Alabama, Inc., United Dental Care of Arizona, Inc., UDC Dental California, Inc., United Dental Care of Colorado, Inc., Union Security DentalCare of Georgia, Inc., United Dental Care of Missouri, Inc., United Dental Care of Michigan, Inc., Union Security DentalCare of New Jersey, Inc., United Dental Care of New Mexico, Inc., UDC Ohio, Inc., United Dental Care of Texas, Inc., United Dental Care of Utah, Inc.. In New York, prepaid dental products are provided by Union Security Life Insurance Company of New York which is licensed in New York and has its principal place of business in Syracuse, New York.