



HIPAA PRIVACY LAWS STRENGTHENED - The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law on February 17, 2009 as part of the American Recovery and Reinvestment Act (ARRA), i.e. the U.S. Stimulus Package.

While most of the HITECH Act has to do with expanding the use of technology in the healthcare industry, it also broadens and strengthens the privacy laws that were originally defined to protect patient health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

In an effort to keep the UTMB faculty and staff well informed of new and emerging compliance requirements, I've put together a condensed version of the HITECH privacy section without all the technical jargon. Please keep in mind that this is only an overview of what I considered as the most significant portion of the Act.

Defines what constitute a security/privacy breach – The Act formally defines what a breach is, but it shouldn't come as any surprise that it's essentially the unauthorized acquisition, access, use, or disclosure of protected health information. There are exceptions to this rule, one being if the acquisition, access or use of PHI was an honest mistake and, upon discovery of the unintended access, the information wasn't further accessed, used or disclosed; and two, if information was unintentionally disclosed, it was only to UTMB colleagues who had similar job duties and access.

Reporting – HIPAA will now require healthcare providers to notify individuals as soon as possible, but no later than 60 days after the discovery of, or what is reasonably believed to be a security breach. If a breach affects more than 500 individuals, notice must be given to prominent media outlets within the region and immediately reported to the Department of Health and Human Services (HHS) where the healthcare providers name will be posted on the HHS website. Breaches involving fewer than 500 individuals will also be reported to the HHS, but may be kept in a log and reported on an annual basis.

Requires an accounting of disclosures at the request of a patient – At the request of an individual, health care providers that use Electronic Medical Records (EMR) must provide an accounting of all disclosures of their protected health information which was made from the EMR during the three years prior to their request. Additionally, individuals have a right to obtain a copy of his or her record in an electronic format or have it sent directly to another recipient.

Imposes restrictions on the disclosures, sales and marketing of protected health information – With the exception of marketing, HIPAA did not restrict healthcare providers from selling Protected Health Information as long as its disclosure was permitted. The HITECH act restricts healthcare providers from receiving monetary compensation in exchange for protected health information unless it is explicitly approved by the individual. Some exceptions to this rule would be public health activities, research, and treatment of the individual. Additionally, at the request of the individual, health care providers are required to restrict the disclosure of their protected health information if; (1) the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment) and (2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

Increases civil monetary penalties for HIPAA violations – Covered entities and persons, i.e. faculty, staff, students, etc. who violate HIPAA regulations due to willful neglect will soon be the subject of civil prosecution and any person who knowingly obtains and/or discloses protected health information without appropriate authorization will be subject to criminal prosecution. Fines can range from \$100.00 – \$50,000.00 per violation depending on the level of severity.

The act also allows for enforcement by State Attorneys General. States may pursue civil action against persons who violates the HIPAA privacy regulations. Fines can range from \$100.00 to 25,000.00, and In

the case of a successful action, the court may also award the costs of the action and reasonable attorney fees to the State.

Impact to UTMB - Because of the work ethics, integrity, professionalism and good judgment of the UTMB staff, most of these changes will not have much of an impact on our work environment or personnel. Some provisions, such as the accounting of disclosure provision, will require our current EMR to be modified to meet that accounting requirements.

With the exception of the increased penalties provision, which is effective immediately, most of the Act's provisions will go into effect in February 2010, others will take longer. Either I, or our Office of Institutional Compliance, will keep you informed of the Acts progress and when provisions become effective.

You can read the privacy section of the HITECH Act in its entirety by going to the [American Recovery and Reinvestment Act \(ARRA\), Subtitle D—Privacy, page 144.](#)

For more information please contact Bob Shaffer at rvshaffe@utmb.edu