THE UNIVERSITY OF CHICAGO
HIPAA Program Office

GUIDANCE March 16, 2010

# KEY PROVISIONS OF THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ("HITECH") ACT RELATED TO HIPAA

In February 2009, the Health Information Technology for Economic and Clinical Health Act ("HITECH") was enacted as part of the American Recovery and Reinvestment Act of 2009 ("ARRA"). HITECH makes significant changes to HIPAA's administrative simplification provisions pertaining to privacy and security, including notifying individuals (and sometimes media outlets) when there has been a privacy/security breach. HITECH's provisions affect not only health care providers, health plans and health care clearinghouses, but a wide range of vendors and contractors that provide services to health care organizations.

**Reporting Security Breaches**
Previously, covered entities (health care providers, health plans and health care clearinghouses) were obligated to mitigate harm caused by unauthorized disclosures of protected health information ("PHI"), but not required to give notice to the individuals whose information was inappropriately disclosed. With HITECH, covered entities and business associates will be required to notify individuals when security breaches occur with respect to "unsecured" information. Unsecured information means information not protected through technology or methods designated by the federal government. In addition, if the breach involves 500 or more individuals, notice to the federal Department of Health and Human Services and the media is also required.

*What is a breach?* Under the HITECH regulations, a "breach" is the unauthorized acquisition, access, use or disclosure of PHI that compromises the security and privacy of the PHI. "Compromise the security and privacy of the PHI" means that the breach poses a significant risk of financial, reputational or other harm to the individual.

*Time Frame.* Covered entities need to notify an individual of a breach of his/her PHI "without unreasonable delay" or no later than 60 days after the breach. A covered entity is considered to have become aware of the breach when the first workforce member or business associate first knew of the breach. *Because of this quick time frame, all UCMC employees and faculty need to be aware of these breach notification provisions and continue to report breaches to the HIPAA Program Office as soon as they are discovered.*

**Under Prior Law, Vendors Not Subject to Privacy Provisions**
Previously, HIPAA applied only to the use and disclosure of PHI by covered entities. Vendors providing administrative services to covered entities, such as legal services, accounting, information technology, financial support and similar services, were not *directly* subject to HIPAA's privacy and security provisions. They were, however, required to sign business associate agreements and thereby agree by contract to maintain the privacy and security of protected health information. Changes made by HITECH expand the scope and application of HIPAA.

**Requirements Expanded to Business Associates**
Among the most far reaching provisions of HITECH are those that apply several of HIPAA's security and privacy requirements to business associates. In addition, business associates will be subject to civil and criminal penalties and enforcement proceedings for violations of HIPAA.

The definition of a business associate is also being expanded to include organizations that provide data transmission of protected health information to covered entities and business associates and that require access on a routine basis to that protected health information. Examples of such organizations include health information exchange organizations, regional health information organizations and vendors that contract with covered entities to provide personal health records.

**Provisions Include Data Restrictions, Disclosure and Reporting Requirements**

*Limited Data Sets*

Currently, covered entities may use and disclose only the "minimum necessary" protected health information for their business purposes, but have considerable latitude to determine what the minimum necessary information is under the circumstances. Under HITECH, covered entities must first consider whether partially de-identified data, known as a limited data set, could be used to accomplish their objectives and must limit their uses and disclosures to limited data sets if possible. A limited data set excludes basic identifying information such as the individual's name, social security number, postal addresses, email addresses, telephone numbers, and similar identifiers.

*Restrictions on Disclosures*

Individuals will be able to bar health care providers from disclosing protected health information to the their health plans if the individuals pay for the health care item or service in full out of pocket.

*Marketing*

The ability of covered entities to use PHI for marketing purposes without the individual's authorization will be limited under HITECH. Specifically, communications with an individual about products or services that encourage the individual to purchase or use the product or service will be permitted without the individual's authorization only if the communication is made (a) to describe a product or service provided by or included in the plan of benefits of the covered entity making the communication, (b) for treatment purposes, or (c) for case management, care coordination, or to recommend alternative therapies, providers, or settings of care. In addition, subject to limited exceptions, the previously described communications will require patient authorization if the covered entity receives direct or indirect payment for making them.

*Accounting of Disclosures*

Covered entities using electronic health records will have to supply individuals with an accounting of disclosures from those records made for treatment, payment, or health care operations purposes during the three years that preceded the request. This will significantly increase administrative burdens for covered entities, which currently are not required to account for such disclosures. This provision is subject to rulemaking and the earliest date it will apply is January 1, 2011.

*Charitable Fundraising*

Health care providers will have to give patients a more conspicuous notice of their option to opt out of receiving charitable solicitations.

*Sales of Protected Health Information*

It will be more difficult for a covered entity to sell electronic PHI without specific patient authorization.

*Enforcement*
HITECH gives power to state attorneys general to bring actions to obtain injunctive relief or damages on behalf of state residents who have been, or are threatened or adversely affected by violations of HIPAA. Previously, HIPAA did not permit individuals to obtain monetary damages for HIPAA violations and enforcement was handled at the federal level. The financial penalties for violations of HIPAA have also been increased significantly, and a percentage of the civil penalties collected will be distributed to individuals harmed by the violations. Outline of updated penalties can be found at http://hipaa.bsd.uchicago.edu/hipaa_background.pdf.

**Effective Dates Vary**
Most provisions will be effective one year after the date of HITECH's enactment (February 17, 2010), however, the security changes will generally be effective 30 days after appropriate regulations are published. The changes to the enforcement provisions are effective for violations occurring after February 17, 2009.