# BREAKING NEWS

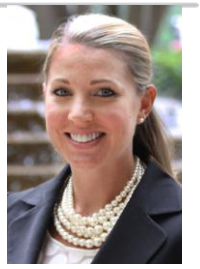
BARNEY&BARNEY LLC

www.barneyandbarney.com

**For Immediate Release:**

January 2013
Employee Benefits
Compliance Breaking News
Volume 2013 Issue 2

**Contact:**
Lisa R. Nelson, Esq.
Director
Compliance & Regulatory Affairs
(858) 875-3017
lisan@barneyandbarney.com



## Final Regulations on HIPAA HITECH Rules Released

The Department of Health and Human Services recently released the long-awaited final regulations on the Health Information Technology for Economical and Clinical Health (HITECH) Act, which modified the Health Insurance Portability and Accountability Act (HIPAA), originally enacted in 2009. Although the final regulations largely reflect the proposed regulations already in effect, some more restrictive elements were added. Highlights are as follows:

### BACKGROUND: FREQUENTLY ASKED QUESTIONS

When does this begin?

- Final rule is effective March 26, 2013 with compliance required by September 23, 2013
- Covered entities and business associates will have until September 22, 2014 to fully amend policies and procedures and business associate agreements and procedures
- Transition provisions: contracts shall be deemed compliant if renewed or modified on or after September 23, 2013 or no later than September 22, 2014

Who does this apply to?

- Covered entities (health plans, health care billing houses, and health care professionals). For health plans that are self-funded, Flexible Spending Accounts (FSA), Employee Assistance Programs (EAP) etc., there is obligation on the employer
- Business associates (entities or persons performing a function for a covered entity that provides access to the covered entity's patients, employee or participant health information)
- Affiliated but legally separate covered entities (i.e., control group entities) may designate themselves as one single affiliated entity for purposes of HIPAA procedures and compliance

What is an employer required to do?

- Covered entities and business associates must update their policies and procedures to reflect the required operational updates
- Covered entities must update business associate agreements with business associates
- Business associates must implement business associate agreements with subcontractors who by way of a service provided to the business associates, has access to Protected Health Information (PHI)
- Conduct a risk assessment/analysis of potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic and other PHI
- Maintain HIPAA policies and procedures, including a sanction policy for workforce HIPAA violations, assignment of security or privacy official responsible for the development and implementation/updating and oversight of HIPAA policies and procedures. Policies should also include termination procedures for

access to electronic Protected Health Information (e-PHI), establishment, review and modification of a user's right to access a workstation, transaction, program or process, identification, response and documentation of suspected or known security incidents (including mitigation of harmful effects)

- Provide periodic evaluations in response to environmental or operational changes
- A covered entity may permit a business associate to create, receive, transmit or maintain PHI only if obtaining satisfactory assurances of the safeguard of the PHI in their care
    - A business associate may permit a subcontractor to do the same
- Train and/or retrain employees in contact with PHI as to the HIPAA privacy and security requirements

What is the penalty?

- $100 per day of violation if the covered entity or business associate did not know it was a violation, up to $1.5 million per violation for knowing and not taking corrective action (willful neglect)

## FINAL REGULATIONS

The HITECH final regulations largely mirror the interim final regulations that have been in play and required compliance beginning in September of 2010. Below, highlights from the final regulations are illustrative of those provisions that experience modifications to the rule since the interim final regulations. For a complete list of all HIPAA privacy and security provisions, including the HITECH rules, see the Barney & Barney (B&B) HIPAA Guidance Manual (available through your B&B representative) and the B&B July 2009 Breaking News.

### Business Associates

- Pursuant to HITECH final regulations, HIPAA privacy and security requirements will now directly apply to business associates
- Business associates may also be liable for the penalties for noncompliance
- Subcontractors of business associates are business associates that must comply with HIPAA privacy and security requirements

### Use and Disclosure Requirements

- PHI regarding deceased individuals no longer protected under HIPAA after 50 years of becoming deceased
- Individuals may prohibit covered entities from sharing PHI concerning treatment if the individual paid for their treatment themselves, in full (e.g., if an individual pays for their treatment in cash, the individual may prohibit the provider from sharing this information with their health plan)
- The sale of an individual's health information for marketing and fund-raising purposes absent their permission is prohibited
    - Marketing does not include communication made to provide a refill reminder, if any financial remunerations received cover the cost of making the communication
- Singular (or compound) authorizations will be permitted for individuals authorizing the use of PHI for research purposes. Psychotherapy notes authorizations may only be combined with other psychotherapy notes authorizations
- Parents and others (guardians or parents acting in loco parentis (legally deemed as acting parent) may give permission to share proof of a child's immunization with a school
- The use or sharing of genetic information is prohibited for underwriting purposes by all health plans, including those to which the Genetic Information Nondiscrimination Act (GINA) does not expressly apply, except with regard to issuers of long term care policies

**Notice of Privacy Practices**

- Notice of privacy practices must be distributed upon service or enrollment in a health plan and then every three years thereafter
    - A health plan that posts the notice on their website must do so prominently and any revised notices with material changes must be posted by the effective date of the change
    - A health plan that does not post notice on their website should provide any revised notice within 60 days of a material change by email, hand-delivery or first-class mail

**Breach Notification Requirements**

- A breach is defined as an impermissible use or disclosure of PHI and is automatically presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised (e.g., the PHI was viewed but information not retained; the PHI was accessed but quickly retraced or computer shut down; or a laptop stolen but encryption made access impossible)
- A business associate must notify the covered entity of a breach of unsecured PHI on the first day of knowing or, by exercising reasonable diligence, would have known of the breach (as discovered by an employee or agent other than the person committing the breach)
- Breach notification required within 60 days where there is a risk of harm. The final regulations modify the terminology to state that breach notification is required where the PHI has been compromised, regardless of the risk of harm
    - Risk of harm analysis is a subjective analysis conducted by the covered entity or business associate
    - Considers probability of inappropriate access to or compromise of PHI considering facts and circumstances of the breach and individuals involved
    - Risk of harm analysis or risk assessment must be documented
    - Breach notification is not required if there is a low probability that the PHI has been compromised

**Request for Access/Copy of Records**

- Patients can request a copy of their electronic medical record in an electronic form. If not possible, then in a readable hard copy form
- Requests for access to one's own PHI in which the covered entity is unable to comply, may only be delayed by 30 days and must be accompanied by a notice of such delay and the reasons why. Only one delay per request is permitted

**Complaints and Compliance Reviews by Health and Human Services**

- Complaints submitted to HHS by the public will be investigated and, where possible, resolved by HHS using informal means of resolution. Informal means of resolution may include the covered entity or business associate demonstrating compliance or a corrective action plan
- Written notice by HHS will be provided informing the covered entity or business associate if the investigation arose from a complaint and that the investigated entity will have the opportunity to submit evidence within 30 days
- A 30-day corrective period will be available even for violations due to willful neglect (beginning on the first day the covered entity or business associate knew or by exercising reasonable diligence should have known of the violation
- If civil monetary penalties are imposed, notice will be provided. Penalty may be waived by HHS if the penalty would be excessive relative to the violation

- Intimidation or retaliation is prohibited
- Affiliated companies are joint and severally liable for civil penalties imposed on one entity in the control group
- A covered entity and business associate is liable for civil monetary penalties for violations based on the act or omission of any agent of the covered entity, including workforce members or business associates, acting within the scope of their job title

## ADDITIONAL INFORMATION

*Employers with self-funded plans, including Employee Assistance Programs (EAP), Flexible Spending Accounts (FSA), Health Reimbursement Accounts (HRA) and Health Savings Accounts (HSA) are required to be HIPAA and HITECH compliant. Barney & Barney clients who have received the B&B HIPAA Guidance Manual will receive an updated manual from their B&B representative once available. The manual should be available by March 15, 2013. The B&B HIPAA Guidance Manual will contain updated HIPAA risk assessments, compliance checklists, model authorization forms, business associate contracts, breach notification forms and tracking sheets, policies and procedures, notice of privacy practices and HIPAA training. Please contact your B&B representative if you are a covered entity in need of HIPAA compliance consultation services. Covered entities and applicable business associates are required to update their policies and procedures. Notice of privacy practices, business associate agreements, authorization forms and risk assessment procedures or checklist must also be updated, in addition to retraining employees in contact with PHI. Compliance is required by September 22, 2014. As mentioned, B&B clients with HIPAA Guidance Manuals will receive all of these required updates from their B&B representative to assist in updating internal processes.*

*HHS News Release, available at:* http://www.hhs.gov/news/press/2013pres/01/20130117b.html
*Final regulations, available at:*
http://www.ofr.gov/(X(1)S(zw1umfg4ni2shu4b1mkmqrt5))/OFRUpload/OFRData/2013-01073_PI.pdf

*For Interim final regulations on breach notifications, see:*
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html*; and,*
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html