BRYAN CAVE
A Broader Perspective

Bulletin

Employee Benefits & Executive Compensation Client Service Group

To: Our Clients and Friends

April 28, 2009

Required Notifications of Breaches of Unsecured PHI Under HIPAA

The American Recovery and Reinvestment Act, also known as the Stimulus Bill, made several changes to HIPAA requirements that are of particular interest to group health plans. Among the changes, HIPAA now requires covered entities, including group health plans, to provide notification to individuals, the Department of Health and Human Services ("HHS"), and, in some cases, media outlets, if *unsecured protected health information* ("PHI") has been breached.

On April 17, 2009, HHS released guidance on how PHI can be protected so it is not considered *unsecured PHI*. Significantly, if PHI is not unsecured PHI, then the breach notification requirements will not apply. This Client Bulletin summarizes certain highlights of this new guidance which may assist you in your compliance efforts.

- Required Notification in the Event of Breaches of Unsecured PHI.
    - If a group health plan has "unsecured protected health information" and there is an unauthorized access, use or disclosure (a "breach") of that information, the group health plan is required to notify the affected individuals.
    - If the plan does not have current or sufficient information to contact 10 or more individuals, then it must post a notice on its website or in major print or broadcast media.
    - If the breach affects 500 or more individuals in a single State or jurisdiction, the notice must be provided in prominent media outlets serving such state or jurisdiction.
    - Plans are required to notify HHS of all breaches. If the breach affects 500 or more individuals (whether or not in a single state or jurisdiction), the notice to HHS must be provided immediately. HHS will post the name of any entity involved in a breach of this size on its website. For smaller breaches, the plan can keep a log of the breaches that it submits to HHS on an annual basis.

- Business associates are required to notify the affected group health plan or other covered entity if they become aware of a breach.
- Notification must be made within 60 days after a breach is discovered.
- Notices to individuals must include the following information:
  - A brief description of what happened, including the date of the breach, if known, and date of the discovery.
  - A description of the types of unsecured PHI that were involved.
  - The steps individuals should take to protect themselves from harm as a result of the breach.
  - A brief description of what the plan is doing to investigate the breach, to mitigate losses and to protect against further breaches.
  - Contact procedures for individuals to ask questions or obtain additional information, including a toll-free number, e-mail address, Web site or postal address.
- These requirements will be effective 30 days after interim final regulations are published. The Act requires that they be published no later than August 16, 2009.

- **Unsecured PHI.**
  - Under the HHS guidance released on April 17th, PHI will not be considered "unsecured," and will therefore not be subject to the notification requirements, if it is rendered "unusable, unreadable, or indecipherable to unauthorized individuals."
  - The guidance identifies two methods by which PHI can be "secured": encryption or destruction.
    - Encryption:
      - The guidance provides that whether or not PHI is properly encrypted depends on the strength of the encryption algorithm and the security of the decryption key or process.
      - The guidance also provides an exclusive list of acceptable encryption methodologies. Methods not specified in the guidance will not be considered sufficient to render PHI "secured."
    - Destruction:
      - Hard copies of PHI will only be considered destroyed if they are unreadable and cannot be reconstructed. Electronic media must be cleared, purged or destroyed consistent with standards described in publications issued by the National Institute of Standards and Technology.

- HHS is also requesting comments on what other methods of encryption or destruction would be acceptable to render PHI "secure." HHS is required to update this guidance no less frequently than annually.

- **More information.**
  - The HHS guidance is available at: www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf
  - The National Institute of Standards and Technology publications referred to in the HHS guidance are available at: http://www.csrc.nist.gov/publications/PubsByLR.html

- **Action Items.**
  - Group health plan administrators and designated HIPAA Privacy and Security Officers should consult with their information technology professionals to determine if their electronic systems on which PHI is stored, used, or destroyed or over which PHI is transmitted comply with the standards set forth in the guidance. They should also review their disposal policies for destroyed hard copies of PHI to ensure the procedures comply with the standards.
  - Group health plan administrators should review and amend their HIPAA policies and procedures to add any necessary standards to keep PHI from being unsecured and to add procedures for complying with the breach notification requirements for any PHI that is considered unsecured.
  - Group health plan administrators should also review and amend their existing business associate agreements to require business associates to provide the information necessary for the plan to satisfy the notice requirement.

Richard (Rick) L. Arenburg	(404) 572-6765	richard.arenburg@bryancave.com
Brian W. Berglund	(314) 259-2445	bwberglund@bryancave.com
Harold G. Blatt	(312) 602-5005	hgblatt@bryancave.com
Armin G. Brecher	(404) 572-6634	armin.brecher@bryancave.com
Bard Brockman	(404) 572-4507	bard.brockman@bryancave.com
Carrie E. Byrnes	(312) 602-5063	carrie.byrnes@bryancave.com
Paul F. Concannon	(404) 572-6856	paul.concannon@bryancave.com
Chad R. DeGroot	(314) 259-2803	chad.degroot@bryancave.com
Edmund (Ed) Emerson	(404) 572-6739	edmund.emerson@bryancave.com
Jennifer Faucett	(404) 572-4516	jennifer.faucett@bryancave.com
Kyle P. Flaherty	(212) 541-2134	kpflaherty@bryancave.com
Mark H. Goran	(314) 259-2686	mhgoran@bryancave.com
Carrie E. Herrick	(314) 259-2212	carrie.herrick@bryancave.com
Castles R. (Cass) Hollis	(404) 572-6923	cass.hollis@bryancave.com
Jonathan Hull	(314) 259-2359	jthull@bryancave.com
Charles B. Jellinek	(314) 259-2138	cbjellinek@bryancave.com
J. Clayton Johnson	(314) 259-2981	jcjohnson@bryancave.com
Hal B. Morgan	(314) 259-2511	hbmorgan@bryancave.com
Dan O'Keefe	(314) 259-2179	dmokeefe@bryancave.com
Michele L. Lux	(314) 259-2519	mllux@bryancave.com
Christian Poland	(312) 602-5085	christian.poland@bryancave.com
Kathy Reardon	(314) 259-2269	kcreardon@bryancave.com
Douglas D. Ritterskamp	(314) 259-2258	ddritterskamp@bryancave.com
Jeffrey S. Russell	(314) 259-2725	jsrussell@bryancave.com
Christopher (Chris) Rylands	(404) 572-6657	chris.rylands@bryancave.com
Michael G. Salters	+44-20-7246-5844	michael.salters@bryancave.com
Steven G. (Steve) Schaffer	(404) 572-6830	steven.schaffer@bryancave.com
Kathleen R. Sherby	(314) 259-2224	krsherby@bryancave.com
Sarah Roe Sise	(314) 259-2741	srsise@bryancave.com
Michael Corey Slagle	(314) 259-2136	corey.slagle@bryancave.com
Richard C. Smith	(602) 364-7395	rcsmith@bryancave.com
Alan H. Solarz	(212) 541-2075	ahsolarz@bryancave.com
Jennifer W. Stokes	(314) 259-2671	jennifer.stokes@bryancave.com
Lisa A. Van Fleet	(314) 259-2326	lavanfleet@bryancave.com
Valerie A. Viemont	(602) 364-7449	vaviemont@bryancave.com
Tom Wack	(314) 259-2182	tewack@bryancave.com
Julie A. Wagner	(314) 259-2637	jawagner@bryancave.com
Qian "Bonita" Wang	(404) 572-6628	q.bonita.wang@bryancave.com
Jay P. Warren	(212) 541-2110	jpwarren@bryancave.com
Carolyn Wolff	(314) 259-2206	carolyn.wolff@bryancave.com
Serena F. Yee	(314) 259-2372	sfyee@bryancave.com