BURR ALERT

EMPLOYER OBLIGATIONS UNDER NEW HIPAA RULES

Action Required by September 23, 2013

With all of the attention garnered by healthcare reform, it would be easy to overlook the new HIPAA rules (the "Rules") applicable to covered entities under HIPAA, which include employer group health plans. Compliance with the Rules is generally required by September 23, 2013. The Rules modify the HIPAA privacy, security, enforcement and breach notification rules by expanding individual rights and strengthening enforcement. The major changes affecting group health plans are summarized below. In addition, health plan documents and SPDs along with HIPAA policies and procedures may need to be updated, and the workforce may need to be retrained in the Rules.

1. **Privacy Notice.** Privacy Notices must be revised to include the following:

   a) A description of the types of uses and disclosures that require an authorization with respect to psychotherapy notes, marketing, and sale of protected health information (PHI);

   b) A statement that other uses and disclosures not described in the Notice will be made only with the individual's written authorization;

   c) If the plan intends to engage in any fund raising activities, a statement that the individual has a right to opt out of receiving such communications;

   d) If the plan intends to use or disclose PHI for underwriting purposes, a statement that it is prohibited from using or disclosing PHI that is genetic information of an individual for such purposes;

   e) A statement that a covered entity (generally a healthcare provider) must agree to a request by an individual to restrict disclosure to the health plan when the individual fully paid for the services out of his own pocket; and

   f) A statement that affected individuals will be notified following a breach of unsecured PHI.

Because HHS considers these changes to be material, it will be necessary to distribute the revised Notice by November 23, 2013. If the Notice is currently maintained on a website, however, the on-line Notice must be updated by September 23, 2013 followed by a hard copy in the next annual participant mailing.

2. **Business Associates and Agreements.** The Rules expand the definition of business associate to include:

a) Those who provide data transmission services and routinely require access to PHI; and

b) Subcontractors, who create, receive, maintain or transmit PHI (all downstream subcontractors, no matter how far down the line).

There is a narrow exception for acting as a "mere conduit." Employers need to review plan service providers not previously identified as a business associate in order to determine if such service providers fall into one of the new categories of business associate.

Business associate agreements need to be updated to include the following provisions (if not already set forth in the agreement):

a) That the business associate agrees to comply with HIPAA security regarding electronic PHI;

b) That the business associate agrees to report any breach of unsecured PHI in accordance with the breach notification rules;

c) That the business associate requires all subcontractors who draft, receive, maintain or transmit PHI on its behalf to agree to the same restrictions and conditions as the business associate; and

d) That the business associate agrees to comply with the privacy rules that are applicable to the covered entity to the extent the business associate is carrying out the covered entity's privacy obligations.

Business associate agreements generally must be updated by September 23, 2013. A transition rule for agreements in place on January 25, 2013 provides additional time for the update, provided that the existing agreement complies with prior requirements and is not renewed between March 26, 2013 and September 23, 2013. Such agreements must be updated by the earlier of the first renewal after September 23, 2013 or September 23, 2014.

3. Liability and Penalties. Business associates (including subcontractors) may now be penalized directly by HHS for many privacy violations. In addition, where a business associate is an agent of the plan, the plan is now liable for violations of the business associate. For this purpose, agency is determined under federal common law under which the key factor is whether the plan has the right or authority to control the business associate's conduct with regard to the services performed on behalf of the plan.

Under the Rules, HHS has less discretion about whether to conduct an investigation, which means more complaints will be investigated, resulting in a greater number of penalties being assessed. The Rules require HHS to investigate complaints when a preliminary review indicates a possible violation due to willful neglect. Willful neglect for this purpose means a conscious, intentional failure or reckless indifference to the obligation to comply. Civil monetary penalties are increased

under a new tiered penalty structure, based on culpability. The penalty ranges from $100 for the lowest tier violation (lack of knowledge) to $50,000 for the highest tier violation (willful neglect), with a maximum penalty of $1.5 million for identical violations in the same calendar year.

4. **Breach Notification.** The Rules modify the definition of breach in a way that serves to expand the circumstances that constitute a breach, replacing the "significant risk" standard with a "compromise" standard. A breach is an acquisition, access, use or disclosure of PHI in a way not permitted by HIPAA that compromises the privacy or security of the PHI. This standard creates a rebuttable presumption where a breach is presumed unless the plan demonstrates that there is a low probability that PHI was compromised, after conducting a risk assessment. The following factors must be included in the risk assessment process:

a) The nature and extent of the PHI involved (including types of identifiers and likelihood of re-identification);

b) The unauthorized person who used the PHI or to whom the disclosure was made;

c) Whether PHI was actually acquired or viewed; and

d) The extent to which the risk to PHI was mitigated.

At the conclusion of the risk assessment, no breach notification is required if the plan determined there was a low probability of the PHI being compromised. The risk assessment process must be documented and the documentation should be maintained.

CONCLUSION

Plans have approximately 6 months to come into compliance with the Rules. HHS has stepped up its audit activity and is assessing penalties on violations. HIPAA compliance is more important now than ever.

If you have any questions or if you would like additional information on this topic, please contact any Burr & Forman attorney listed below.

C. LOGAN HINKLE
Partner ~ Birmingham
(205) 458-5154
lhinkle@burr.com

HOWARD BOGARD
Partner ~ Birmingham
(205) 458-5416
hbogard@burr.com

KELLI FLEMING
Partner ~ Birmingham
(205) 458-5429
kfleming@burr.com

DEBRA MACKEY
Counsel ~ Birmingham
(205) 458-5484
dmackey@burr.com

JAMES HOOVER
Partner ~ Birmingham
(205) 458-5111
jhoover@burr.com