How the Final HIPAA Regulations Impact Group Health Plans

The U.S. Department of Health and Human Services ("HHS") recently issued final regulations ("Final Rule") modifying the privacy, security, enforcement, and breach notification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and implementing the Health Information Technology for Economic and Clinical Health ("HITECH") Act.

Employer-sponsored group health plans ("GHPs") are HIPAA-covered entities that must comply with the Final Rule. The most significant changes impacting GHPs are: (1) the new definition of "breach" under the breach notification provisions; (2) new required content for business associate agreements; (3) the imposition of vicarious liability for acts of business associates; and (4) new required content and distribution requirements for notices of privacy practices.

1. The New Definition of "Breach"

HIPAA's privacy rules restrict the use and disclosure of protected health information ("PHI"). A GHP may inadvertently disclose a participant's PHI if, for example, the GHP inadvertently emails PHI to the wrong employee or posts a participant's PHI on the plan's benefits website.

In 2009, the HITECH Act added breach notification provisions to HIPAA. Under these rules, a GHP must promptly notify participants and HHS if a participant's unsecured PHI is disclosed due to a breach. "Breach" was defined as the unauthorized acquisition, access, use, or disclosure of PHI that poses a significant risk of financial, reputational, or other harm to the individual. This "harm" threshold was widely viewed as subjective and causing the underreporting of PHI breaches.

The Final Rule eliminates the harm threshold and greatly expands the definition of breach. A GHP must now presume its disclosure of unsecured PHI caused a breach, unless the plan can demonstrate that there is a "low probability" that the PHI has been compromised. The new "low probability" standard requires an affected GHP to perform a risk assessment that takes into account the following factors:

a. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
b. the unauthorized person that used the PHI or to whom the disclosure was made;
c. whether the PHI was actually acquired or viewed; and
d. the extent to which the risk of further impermissible use or disclosure of the PHI has been mitigated.
GHPs have the burden of proving that there was a low probability of a breach or, if not, that all notices of the breach were provided. Therefore, all risk assessment documentation and notices should be retained. GHPs will be required to report breaches more frequently under the broader breach definition. To ensure compliance, plan sponsors should review their breach reporting policies and procedures and, as discussed below, update their business associate agreements accordingly.

2. Business Associate Agreements

HIPAA regulations allow a GHP to disclose participant PHI to business associates, such as third-party administrators and vendors, if the GHP obtains “satisfactory assurances” in a written contract (“business associate agreement” or “BAA”) that business associates will protect participant PHI. The Final Rule modifies the required content for BAAs. BAAs must now provide that business associates will:

a. use appropriate safeguards to prevent illegal use or disclosure of electronic PHI;
b. report to the GHP any use or disclosure inconsistent with the BAA that the business associate becomes aware of and report breaches of unsecured PHI (see above);
c. ensure its subcontractors agree to the same restrictions and conditions as the business associate; and
d. comply with the HIPAA privacy rule requirements to the extent the GHP delegates its obligations.

Consistent with requirements of (c) and (d) above, the Final Rule revises the definition of “business associate” to include subcontractors and makes business associates directly liable for certain HIPAA violations (in addition to contractual liability to the GHP under the BAA). The Final Rule also eliminates the requirements that GHPs report material BAA breaches to HHS where the business associate cannot cure the breach and BAA termination is infeasible. The preamble to the Final Rule explains the requirement was removed because HHS has “other mechanisms” to learn of breaches and PHI misuses. Specifically, the preamble points out that GHPs and business associates are already required to report breaches of unsecured PHI to HHS, and business associates are directly liable for certain HIPAA violations under the BAA.

A model agreement and a full list of the BAA content requirements are available on the HHS website (http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html). BAAs must generally comply with the Final Rule's BAA content requirements by September 23, 2013, except that agreements in place as of January 25, 2013 that are not renewed or modified between March 26 and September 23, 2013 are deemed compliant until September 22, 2014, provided the agreement continues not to be renewed or modified.

3. Vicarious Liability for Business Associates

In addition to the specific BAA content requirements, there is another significant issue to keep in mind when reviewing BAAs. Previously, GHPs were generally not liable for actions of their business associates if they entered into a compliant BAA. Under the Final Rule, however, GHPs are liable for the acts or omissions of business associates that are acting as their “agents.” For example, a GHP that delegates breach reporting obligations to a business associate could be held vicariously liable, if the business associate is an agent and fails to report a breach. To determine whether a business associate is an agent, HHS will examine the BAA and evaluate whether the plan sponsor:

a. retains authority to give the business associate interim instructions;
b. can direct how the business associate performs a service after the agreement is signed; and
c. delegates HIPAA obligations to the business associate.
On the other hand, the preamble to the Final Rule notes that a business associate is not an agent if the only way the plan sponsor can control the business associate's actions is through the BAA (i.e., by amending the agreement or suing for breach).

If an agency relationship exists, to avoid vicarious liability, plan sponsors could:

a. eliminate the agency relationship by either (i) amending the BAA to assume the HIPAA obligation themselves; or (ii) relinquish their control over the business associate for a delegated HIPAA duty such that the only way to control the business associate's actions is by enforcing the BAA; or

b. retain the provision triggering the agency relationship, but ensure that the business associate complies with HIPAA by adding detailed provisions regarding HIPAA compliance and/or a provision requiring the business associate to indemnify the GHP for any vicarious liability.

In sum, plan sponsors should scrutinize their BAAs to determine which services may trigger an agency relationship with the business associate and, if triggered, contemplate the modifications proposed above.

4. Notice of Privacy Practices

GHPs routinely include a HIPAA Notice of Privacy Practices (“NPP”) in their open enrollment materials. The Final Rule requires that a NPP include:

a. a description of activities involving PHI uses and disclosures that require a participant’s authorization (e.g., using psychotherapy notes, and disclosures for marketing purposes and that constitute the sale of PHI);

b. a statement reflecting that any other PHI uses or disclosures not described in the NPP will be made only with the participant’s authorization;

c. a basic statement that GHPs are legally required to notify individuals if their unsecured PHI is breached (see above); and

d. if the GHP intends to use participant PHI for underwriting purposes, a statement that the plan is prohibited from using or disclosing genetic information.

As requirement (d) highlights, the Final Rule prohibits GHPs from using or disclosing PHI that is genetic information for underwriting purposes, consistent with the Genetic Information Nondiscrimination Act of 2008 (“GINA”).

The Final Rule also amends the NPP distribution requirements. Previously, GHPs were required to distribute their privacy notices within 60 days of a material revision. Under the Final Rule:

a. If the GHP posts the NPP on its website, then it must:

i. prominently post the material changes to the NPP, or the revised NPP itself, on its website by the material change's effective date (i.e., September 23, 2013); and

ii. provide information about the material changes to the NPP and how to obtain the revised NPP, or send the revised NPP itself, in the next annual mailing to participants (e.g., beginning of the plan year or open enrollment).

b. If the GHP does not post the NPP on its website, then the plan must provide information about the material changes to the NPP and how to obtain the revised NPP, or the revised NPP itself, to participants within 60 days of the material revision (i.e., November 22, 2013 for employers that wait until the September 23, 2013 deadline to revise their NPPs).

HHS has determined that these new provisions materially change the NPP. Thus, GHPs should begin revising their NPPs so that they are ready to be distributed by the applicable deadline.
Conclusion

GHPs generally have until September 23, 2013 to comply with the Final Rule, except as noted above for BAAs and hard-copy NPPs. GHPs should heed these deadlines because the Final Rule significantly increases civil penalties for HIPAA violations based on culpability level, and mandates HHS investigations and compliance reviews for possible violations due to willful neglect. Plan sponsors should review their breach notification procedures, BAAs, NPPs, and other HIPAA practices and documents to ensure that they are prepared for an HHS audit.

If you have any questions about this memorandum, please contact Mark Burgreen in our Syracuse office ((315) 218.8279, mgburgreen@bsk.com) or any of the other members of our Employee Benefits and Executive Compensation Practice Group listed below.

Albany: (518) 533-3000
   Amelia M. Klein   aklein@bsk.com

Buffalo: (716) 566-2800
   John C. Godsoe   jgodsoe@bsk.com
   Daniel R. Sharpe  dsharpe@bsk.com

Long Island: (516) 267-6300
   Terry O'Neil     toneil@bsk.com

New York City: (646) 253-2300
   Michael P. Collins  mcollins@bsk.com

Rochester: (585) 362-4700
   James Holahan    jholahan@bsk.com

Syracuse: (315) 218-8000
   Stephen C. Daley sdaley@bsk.com
   Brian K. Haynes   bhaynes@bsk.com
   Richard D. Hole   rhole@bsk.com
   Ted Lewkowicz    tlewkowicz@bsk.com
   Aaron M. Pierce  apierce@bsk.com