D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

AUGUST 2009

BENEFITS & COMPENSATION
>> ALERT

HIPAA IN A "HITECH" WORLD

Is your organization ready to comply with the new HIPAA breach notification rules?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires certain covered entities and their business associates to protect the privacy and security of individually identifiable health information (protected health information, or PHI). Covered entities include health plans and certain health care providers. Business associates are those entities that perform activities on behalf of a covered entity that involve the use or disclosure of PHI (e.g., medical claims administration services involving the use of PHI).

NEW LEGISLATION & GUIDANCE

Recent legislation known as "HITECH" significantly changes the HIPAA rules. The first of these changes to be effective provides that HIPAA covered entities and their business associates must now provide notice to affected individuals and other parties in the event of a privacy breach. The Department of Health and Human Services (HHS) published guidance on August 24, 2009 addressing these new breach notification rules, which are effective September 23, 2009.

ACTION STEPS

Covered entities, including employers that sponsor health plans, and their business associates must, within a very short time frame, take action to comply with the new HIPAA breach notification rules, including some or all of the following:

>> If your organization sponsors a health plan, understand that you must ensure that your plan complies with HIPAA, including the new breach notification rules

>> If your organization is a business associate of a covered entity, understand that HITECH directly changes how your organization must comply with HIPAA, including the new breach notification rules

>> Review your overall HIPAA compliance effort and, if feasible, de-identify, encrypt or destroy PHI (or avoid/minimize handling PHI altogether)

THE BOTTOM LINE

The Department of Health and Human Services published guidance on August 24, 2009 addressing new HIPAA breach notification rules, which are effective September 23, 2009. HIPAA covered entities, including employers that sponsor health plans, and business associates of covered entities, must immediately assess their HIPAA compliance efforts or risk having to notify individuals, the government and media outlets in cases of privacy breach.

>> Implement written policies and procedures addressing the new HIPAA breach notification rules

>> Create a system to log incidences of privacy breaches

>> Review and, if appropriate, revise business associate agreements to address the new breach notification rules

>> continues on next page

- Train workforce members on the breach notification rules
- Review and update contact information for those individuals whose PHI you handle (or face substitute notice requirements through media outlets)
- Respond to suspected privacy breaches by determining and documenting:
  - whether there has been an impermissible use or disclosure of PHI under the Privacy Rule
  - whether the impermissible use or disclosure compromises the security or privacy of the PHI (i.e., whether there is a significant risk of financial, reputational, or other harm to the individual)
  - whether the incident falls under one of the exceptions to the breach definition
  - provide any required breach notifications within applicable time frames.

BREACH NOTIFICATION APPLIES TO UNSECURED PHI

Notification is required when there is a breach of PHI that is deemed to be "unsecured." Notification is not required when there is a breach of PHI that is secured—however, encryption and destruction are presently the only two technologies and methodologies that are sufficient to secure PHI for purposes of the breach notification rules. All other PHI (e.g., PHI in written form; unencrypted electronic PHI), therefore, will be deemed unsecured and subject to the breach notification rules.

BREACH DEFINED

The guidance specifies that "breach" means "the acquisition, access, use, or disclosure of PHI in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the PHI." Under this definition, therefore, not all violations of the Privacy Rule will require notification. Specifically, in order for there to be a breach requiring notification, the impermissible use or disclosure must pose "a significant risk of financial, reputational, or other harm to the individual." Thus, each time there is a breach, a risk assessment must be performed to determine if there has been sufficient harm to the individual requiring notice.

RISK ASSESSMENT

Among other items, HHS specifies that the risk assessment must be documented and should be fact specific and consider that many forms of health information are sensitive for purposes of the risk of reputational harm. Immediate steps taken to mitigate an impermissible use or disclosure may reduce the risk of harm to the individual to a less than "significant risk."

EXCEPTIONS TO BREACH

The guidance provides exceptions, where notice is not required, including that there is no breach when there is:

- an unintentional, otherwise good-faith, breach by a workforce member of a covered entity or business associate that does not result in further improper use or disclosure of the PHI
- an inadvertent disclosure from one authorized person to another within a covered entity or business associate that does not result in further improper use or disclosure of the PHI
- an impermissible disclosure where the recipient would not have been able to retain the information.

>> continues on next page

BREACH NOTIFICATION

The HHS guidance addresses notification to various parties, including the following:

(1) Notification to an individual

>> *Timing.* Notice must be provided to the individual "without unreasonable delay" and in no case later than 60 days after discovery of a breach.

>> *Content and form of notice.* The notice should be written in plain language and describe the date of breach and date of discovery; the type of PHI breached; any steps individuals should take to protect themselves from harm and steps the covered entity is taking to investigate the breach, to mitigate harm to individuals, and to protect against future breaches. Notice must be provided by first-class mail to the last known address of the individual. E-mail notification is not allowed, except where the individual has previously agreed to such notice.

>> *Incorrect addresses will require substitute notice.* Substitute notice (e.g., telephone, e-mail, posting, in certain cases) must be provided if the covered entity has insufficient or out-of-date contact information for one or more affected individuals. If this relates to 10 or more individuals, then substitute notice must be provided through either a conspicuous posting for a period of 90 days on the home page of the covered entity's web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.

(2) Notice to Media of a Breach of Unsecured PHI of 500 State Residents

Notice must be provided to prominent media outlets serving a state or jurisdiction following the discovery of a breach involving the unsecured PHI of more than 500 residents of state or jurisdiction.

(3) Notification to Secretary

Notice must be provided to the Secretary of HHS at the time notice is provided to individuals for breaches involving 500 or more individuals. For breaches involving less than 500 individuals, a log of these breaches must be maintained and submitted annually to the Secretary.

(4) Notification by Business Associate to Covered Entity

A business associate that discovers a breach of unsecured PHI must provide notice to the covered entity without unreasonable delay and in no case later than 60 days after discovery. As with the covered entity, a breach is treated as discovered as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known.

SANCTIONS WILL NOT APPLY FOR 180 DAYS

HHS will not impose sanctions for failure to provide the required notifications for breaches that are discovered before February 22, 2010. Nevertheless, during this initial time period, HHS expects covered entities to comply with the new guidance and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance.

FOR MORE INFORMATION

Mark E. Bokert
Partner/Chair
212.468.4969
mbokert@dglaw.com

Alan Hahn
Partner
212.468.4832
ahahn@dglaw.com

or the D&G attorney with whom you have regular contact.

DAVIS & GILBERT LLP
T: 212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com