GRAY • PILGRIM

AND ASSOCIATES, LLC

August 13, 2013

Dear Client,

The Department of Health and Human Services Office for Civil Rights has issued some major changes to the Health Insurance Portability and Accountability Act commonly known as HIPAA. There are some changes you will need to make immediately and some you need to be working towards.

There has been an expansion of the definition of Business Associates to include subcontractors that access Personal Health Information (PHI). There is now a direct liability on Business Associates for compliance. Covered entities and Business Associates have until the due date of September 23, 2013 to comply with these updated provisions. All Business Associate Agreements must be revised to be compliant with these new requirements by the **September 23, 2013** deadline, except that there are grandfathering provisions for certain existing Business Associate Agreements. Those Business Associate Agreements in existence as of January 23, 2013 that meet all of the HIPAA Security and Privacy Rule requirements, and are not renewed or modified between March 25, 2013 and September 23, 2013, may have an additional year to comply. That puts the date to September 22, 2014.

There are new disclosures that need to be made in informing individuals of their right to be notified of breaches of their Personal Health Information (PHI). There has also been a substantial lowering of the threshold for notification of affected individuals in the event of a breach of PHI and a requirement to conduct a documented risk assessment in the event notification is not provided in reliance on the harm threshold and the expansion of individuals' rights to access their PHI.

Here are some highlights of the changes:

Privacy Practices – Covered Entities must revise their Notice of Privacy Practices. It should address certain uses and disclosures that require authorization. It must tell the individual they have a right to be notified following a breach of their unsecured PHI. Authorization is required for most uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of PHI. It must also address that the individual has the right to opt out of fundraising communications if the covered entity intends to use PHI for fundraising. The individual can restrict certain disclosures of PHI to a health plan if the individual pays out of pocket in full for the

service. Uses and disclosures not described in the Privacy Notice will be made only with the authorization from the individual.

Individuals Access to the PHI – If an individual requests a copy of their PHI that you have in electronic format, you must provide them with access to that in a format as they request. If you cannot readily produce it in that format, you must produce a readable electronic copy. If the information isn't readily producible in the format they requested, and you maintain records on paper, then you must produce a readable hard copy. You can only charge for labor costs for copying the PHI requested by the individual whether in paper or electronic form and cost of supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media and postage when the individual has requested the copy or the summary or explanation be mailed and preparing an explanation or summary of the PHI if agreed to by the individual as required. The second aspect of this is when an individual requests that their PHI be sent to a designated third party, you must send the information to that third party; however, the individual no longer has to fill out and sign a "HIPAA compliant" authorization form. They need only sign a written request that defines to whom and where the PHI should be sent.

You are permitted to disclose PHI to the individual, or for their treatment, payment or healthcare operations or when there is a valid authorization or by agreement as permitted.

HIPAA rules deem the revisions to HIPAA Privacy Policy Notices are material and therefore require redistribution of the updated HIPAA Privacy Notices. The existing rules say that covered entities must prominently post the revised Privacy Notice on their site by the effective date of the changes (September 23, 2013), and also provide the revised Privacy Notice in the covered entity's next annual mailing to affected individuals. If the notice is not provided via a website, the covered entity must provide it to affected individuals within 60 days of the effective date of the updated notice.

Business Associate - Revisions to your Business Associate Agreements should be made. Business Associates and their subcontractors are not DIRECTLY LIABLE to Department of Health and Human Services (DHHS) for compliance with HIPAA safeguards and breach notification. Business Associates are no longer "only" contractually liable to Covered Entities, and must implement their own policies and procedures complying with the new rules. Business Associates are directly liable for the use or disclosure of PHI that is not permitted in its Business Associate Agreement or by the Privacy Rule. This is a dramatic expansion of their liability. They are directly liable for failure to comply with Security Rule obligations and requirements as well as the failure to make reasonable efforts to limit PHI to the minimum necessary as well as failure to enter into business associate agreements with subcontractors that are also business associates. This is an expansion in the definition of Business Associates as it includes subcontractors that access PHI.

A Business Associate is anyone who creates, receives, maintains, or transmits PHI for a function regulated by the rules. Vendors that require routine or more than random access to PHI are Business Associates and those that act as mere conduits for or have random access to PHI continue to be outside the scope of the definition. Business Associates include claims processors, administrators, data analysts,

individuals or entities performing quality assurance activities, and persons conducting patient safety activities. Now included are those that perform legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a Covered Entity if that service provided involves any disclosure of PHI. Health information organizations, e-prescribing gateways and anyone who provides data transmission services with respect to PHI to a covered entity and that required access on a routine basis to PHI is considered a business associate. A subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate is considered a business associate. Data storage or document storage vendors whether or not they view the PHI they maintain are deemed to be Business Associates. Operators of portals or other interfaces created on behalf of covered entities that allow patients to share their date with the covered entity are considered Business Associates. Note, that an employee of the practice is not considered a business associate. A healthcare provider or a government agency or a plan sponsor with respect to disclosures by a group health plan to the plan sponsor is not considered a business associate either.

Immunization Records – A covered entity may now release student immunization records without having a patient authorization as long as the state law requires the school to have the immunization record and the covered entity can document that it has oral or written agreement from the individual or their parent or legal guardian for the disclosure.

Decedents – An individual's personal health information is no longer considered to be PHI 50 years after death. A covered entity can now disclose PHI to persons involved in the decedents care or payment as long as it is not contrary to the individual's prior expressed preference. The disclosure is still what is minimally necessary to be disclosed.

Notification of Breaches – HIPAA rules introduce comprehensive updates to the requirements governing the investigation and response to potential breaches of electronic PHI. A breach is defined as an unauthorized acquisition, access, use, or disclosure of PHI in a manner that is not permitted by HIPAA and that it compromises the security or privacy of the PHI. Breach excludes any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure. A breach also excludes any disclosure from one authorized person to another authorized person and it also excludes a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Previously, the rules required a risk assessment for determining the "risk of harm" to the individual. This was a process where you determined whether there was a breach and if notice needed to be provided. That assessment is now essentially gone, because now if any such unauthorized use or disclosure occurs, it is considered a breach unless you can demonstrate that there is low probability that the PHI has been compromised based on a risk assessment.

To complete a documented risk assessment you have to look at four factors. One is the nature, extent type and sensitivity of the PHI; two the unauthorized person who used the PHI or to whom the PHI was disclosed; three is whether the PHI was actually received or viewed or merely subject to the opportunity for such access and four, the extent that the risk to the PHI has been mitigated including efforts to obtain assurances that the PHI will not be further used or disclosed, and the reliability of such efforts under the circumstances. The burden of proof for not providing notification following and based on the risk assessment still is made on the Covered Entity.

If however, the Covered Entity decides to notify the individual that there was a breach, then you don't have to perform the risk assessment.

The timeline for notification of breaches to the DHHS affecting less than 500 people is within 60 days of the end of the calendar year in which the breach was discovered.

Enforcement and Penalties – The Office of Civil Rights (OCR) now is required to investigate any HIPAA complaint received when a preliminary review of the facts shows that there is a possible violation due to willful neglect. Willful neglect for this purpose is defined to mean conscious, intentional failure or reckless indifference to the obligation to comply with HIPAA. OCR will now also conduct compliance reviews to determine whether a covered entity or business associate is complying with the HIPAA rules.

Civil Monetary Penalties – If the Secretary determines that the covered entity or business associate has violated an administrative simplification provision then a civil money penalty will be levied. Restated, an administrative simplification provision is any such requirement under HIPAA.

Where there is a violation in which it is established that the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, that the covered entity or business associated violated a provision, there is a penalty of not less than $100 per violation or more than $50,000 for each violation with an annual maximum of $1.5 million dollars.

Where there is a violation in which it is established that the violation was due to reasonable cause and not willful neglect, the penalty will be not less than $1,000 or more than $50,000 for each violation with an annual maximum of $1.5 million dollars. Reasonable cause for this means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

Where there is a violation in which it is established that the violation was due to willful neglect and was timely corrected, the penalty would be not less than $10,000 or more than $50,000 for each violation. Willful neglect in this exercise means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

Lastly, when there is a violation in which it is established that the violation was due to willful neglect and was not timely correctly, a penalty of not less than $50,000 for each violation , except that a penalty for

violations of the same requirement or prohibition under any of these categories may not exceed 1.5 million dollars. There are different penalty amounts for repeat violators.

As you can tell, this is a multi-layered issue to be taken seriously and there are new enforcement and punitive measures in place. It can be confusing, but understanding and compliance are crucial. This article is not meant to be comprehensive or conclusive, just a reminder that every practice needs to take action. This is an area where we strongly encourage that you work with a healthcare attorney who is experienced in this subject and can help you both insulate and position your practice properly. Once you have the proper documents in place, you must educate your staff regularly and monitor this area on an ongoing basis in order to be compliant.