PULLMAN & COMLEY, LLC
ATTORNEYS AT LAW

# HEALTH CARE LAW ALERT

This alert is written by Jennifer Willcox, attorney in the Health Care Department at Pullman & Comley, LLC. Please feel free to contact Jennifer or any of the attorneys listed below for more information.

| | | |
|---|---|---|
| Collin P. Baron | 203-330-2219 | cbaron@pullcom.com |
| Rebekah M. Burgio | 203-254-5011 | rburgio@pullcom.com |
| Bonnie L. Heiple | 860-424-4355 | bheiple@pullcom.com |
| Nancy D. Lapera | 203-330-2107 | nlapera@pullcom.com |
| Michael N. LaVelle | 203-330-2112 | mlavelle@pullcom.com |
| Elliott B. Pollack | 860-424-4340 | ebpollack@pullcom.com |
| Michael G. Proctor | 203-330-2145 | mproctor@pullcom.com |
| Jennifer N. Willcox | 203-330-2122 | jwillcox@pullcom.com |

This alert is intended for educational and informational purposes only. Readers are advised to seek appropriate professional consultation before acting on any matters in this update. This report may be considered advertising. To be removed from our mailing list, please email unsubscribe@pullcom.com, with "Unsubscribe" in the subject line. Prior results do not guarantee a similar outcome.

NOVEMBER 2009

## Breach Notification Regulations and Increased HIPAA Penalties Under HITECH: Health Care Providers, Plans and Vendors Must Comply

Under the Health Information Technology for Economic and Clinical Health Act, (the HITECH Act), part of the massive stimulus bill passed early in the Obama administration, Congress made a number of changes to the HIPAA Privacy and Security rules. These changes include increasing the penalties that can be imposed and charging the federal Department of Health and Human Services (HHS) with issuing regulations requiring HIPAA-covered entities and business associates to notify patients when their "unsecured" protected health information (PHI) has been used or disclosed improperly. HHS issued these "breach notification" regulations on August 23, 2009, and the regulations were effective September 23, 2009, (although HHS has indicated it will not impose sanctions before February 22, 2010). Covered entities and their business associate service providers should carefully review their privacy and security policies and consider how they will comply with these breach notification requirements.

The breach notification regulations require all HIPAA-covered entities to provide notification to all affected individuals and to the Secretary of HHS after the discovery of a breach of unsecured PHI. Depending on the number of individuals involved, covered entities sometimes may be required to provide notification of the breach to the media or to HHS. If a business associate of a covered entity experiences a breach, the business associate must notify the covered entity, including the identification of each potentially affected individual. HHS also must post to its website a list of covered entities that experience breaches of unsecured PHI involving more than 500 individuals, and covered entities must report annually to HHS regarding all breaches of unsecured PHI.

The current regulations provide some exceptions to what constitutes a "breach," and breach notification is triggered only if the covered entity determines that the use or disclosure “poses a significant risk of financial, reputational or other harm to the individual.” The regulations also include requirements on the timing and content of breach notices, and guidance on how PHI can be “secured” (and therefore not subject to the breach notification regulations). The breach notification regulations are considered “interim” final regulations and HHS took comments until October 23, 2009; whether the agency will make any significant changes remains to be seen.

On October 30, 2009, HHS issued yet another "interim final rule," this one relating to the increased penalties for HIPAA violations imposed by the HITECH Act. Prior to the HITECH Act, the maximum penalty for each HIPAA violation was $100, and the maximum penalty for all violations of an identical requirement was $25,000. In addition, if the Office for Civil Rights (OCR) sought to impose a penalty, but the covered entity could show that it did not know, or by reasonable diligence could not have known, of the violation, then the covered entity has a complete defense to any penalties. Critics charged that OCR was lax in enforcing HIPAA, and in five years of HIPAA oversight OCR had not imposed a single monetary penalty for HIPAA violations.

The HITECH Act changed the penalty scheme, and both covered entities and business associates are now subject to much larger penalties for violations occurring after February 18, 2009, under four different categories of violations. For violations about which the covered entity did not know, or by reasonable diligence could not have known, the penalty range for each violation is $100 to $50,000. For violations due to reasonable cause and not to willful neglect, the penalty range for each violation is $1,000 to $50,000. For violations due to willful neglect that are corrected within 30 days, the penalty range for each violation is $10,000 to $50,000. And for violations due to willful neglect that are not corrected within 30 days, the minimum penalty is $50,000. For all categories of violations, the maximum penalty amount that may be imposed for identical violations in a calendar year is $1.5 million. For violations in the first two categories, correction within 30 days can be a way to avoid the imposition of penalties altogether. Judging from some recent pronouncments, OCR enforcers likely will be much more aggressive in imposing penalties than they have in the past.

Covered entities and business associates are advised to understand these requirements and develop policies and procedures for compliance. Covered entities and vendors to the health care industry also will want to consider revising their business associate agreements to address breach notification and the other HIPAA changes in the HITECH Act. Attorneys in Pullman & Comley’s Health Care Department can help you understand the evolving HIPAA requirements and develop appropriate strategies to ensure compliance.