

September 18, 2009

New Health Plan Privacy Notice Requirements Under HITECH Act

The Department of Health and Human Services (“HHS”) recently issued an interim final rule (the “Rule”) under the Health Information Technology for Economic and Clinical Health (“HITECH”) Act explaining the notification requirements for breaches of protected health information that has not been encrypted or destroyed (“Unsecured PHI”). Employer-sponsored health plans should immediately review and revise their HIPAA privacy policies and procedures to ensure that they adequately address the Rule’s requirements for investigating and reporting breaches of Unsecured PHI. The new requirements are effective for breaches occurring on or after September 23, 2009.

“Covered entities,” including group health plans, must notify affected individuals, the Secretary of HHS, and in some cases, the media, following the discovery of a breach of Unsecured PHI. The notice should be delivered by first-class mail, or by e-mail, if the individual has agreed to accept electronic notices and should include: a description of the breach, steps individuals should take to protect themselves, steps the covered entity is taking in response to the breach, and contact information for individuals to obtain more information. In cases where individuals cannot be reached, notices may be posted on the covered entity’s website, or announced in major print or broadcasting media. Where the breach involves more than 500 residents of a state or jurisdiction, the covered entity must also provide notice to prominent media outlets in that state or jurisdiction. Notices generally must be delivered within 60 calendar days after the discovery of the breach.

If a breach occurs at or by a covered entity’s “business associate”, the business associate must notify the covered entity of the breach. This notice must identify, to the extent possible, the individuals whose Unsecured PHI was subject to the breach and include the information required to be included in the notice sent by the covered entity.

The Rule imposes sanctions for failure to deliver notices when the covered entity or business associate would have known of a breach by exercising reasonable diligence, even if the covered entity or business associate did not actually know of the breach. Therefore, it is critical that (i) covered entities and business associates have procedures in place to effectively discover breaches and to investigate and report breaches when they occur, and (ii) all individuals acting on their behalf are trained to comply with these procedures.

If you have any questions regarding the foregoing, please contact one of the attorneys listed below.

[Charles F. Plenge](#)

214.651.5573

charles.plenge@haynesboone.com

[John M. Collins](#)

214.651.5564

john.collins@haynesboone.com

[Greta E. Cowart](#)

214.651.5592

greta.cowart@haynesboone.com

[Jesse J. Gelsomini](#)

713.547.2233

jesse.gelsomini@haynesboone.com

[Susan A. Wetzel](#)

214.651.5389

susan.wetzel@haynesboone.com

[Marilyn C. Doolittle](#)

713.547.2901

marilyn.doolittle@haynesboone.com

[Tiffany Walker](#)

512.867.8455

tiffany.walker@haynesboone.com

[James Williamson](#)

214.651.5224

james.williamson@haynesboone.com

[Kirsten H. Garcia](#)

214.651.5171

kirsten.garcia@haynesboone.com

[Katy B. Zarolia](#)

214.651.5121

katy.zarolia@haynesboone.com

[Chris M. Kang](#)

214.651.5944

chris.kang@haynesboone.com

[Nellie Strong](#)

214.651.5447

nellie.strong@haynesboone.com

[Brian K. Giovannini](#)

713.547.2025

brian.giovannini@haynesboone.com

haynesboone.com

Austin Dallas Fort Worth Houston Mexico City Moscow New York Orange County Richardson San Antonio San Jose Washington, D.C.