Curran Tomko Tarski LLP

2001 BRYAN STREET, SUITE 2050, DALLAS, TX 75201 TEL: 214.270.1400 FAX: 214.270.1401

Latest in Health Care

HHS Delegates Authority for the HIPAA Security Rule to Office for Civil Rights

August 3, 2009

The Department of Health & Human Services (HHS) yesterday (August 3, 2009) transferred authority for the administration and enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule to the Office for Civil Rights (OCR). Prior to this announcement, responsibility for interpretation and enforcement of the Security Rule rested with the Centers for Medicare & Medicaid Services (CMS). The change reflects the growing seriousness of HHS and others about enforcing federal privacy and data security mandates for health information. HHS anticipates the transfer of authority will eliminate duplication and increase efficiencies in how the department ensures that Americans' health information privacy is protected.

HHS has the authority for administration and enforcement of the federal standards for health information privacy called for in HIPAA. The Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. OCR has been responsible for enforcement of the Privacy Rule since 2003. The Security Rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA), mandated improved enforcement of the Privacy Rule and the Security Rule.

Through a separate delegation, CMS continues to have authority for administration and enforcement of the HIPAA Administrative Simplification regulations, other than privacy and security of health information.

The transfer of Security Rule enforcement authority comes as guidance about new data breach rules for electronic protected health information is impending. This impending guidance relates to the implementation of new breach notification rules for covered entities and their business associates concerning their obligation to use technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, as required by amendments to HIPAA enacted under the HITECH Act. OCR officials have stated that they are working to publish the next set of regulations regarding these new breach notifications before the end of August, 2009.

In addition to adding the breach notification requirements, the HITECH Act also tightened the HIPAA mandates in several other respects. Among other things, it amended HIPAA to:

- Broaden the applicability of the HIPAA's Privacy Rules and penalties to include business associates;
- Clarify that HIPAA's criminal sanctions apply to employees or other individuals that wrongfully use or access PHI held by a covered entity;
- Increase criminal and civil penalties for HIPAA Privacy Rules violators;
- Allow State Attorneys General to bring civil damages actions on behalf of certain state citizens who are victims of HIPAA Privacy and Security Rule violations;
- Modify certain HIPAA use and disclosure and accounting requirements and risks;
- Prohibits sales of PHI without prior consent;

- Tighten certain other HIPAA restrictions on uses or disclosures;
- Tighten certain HIPAA accounting for disclosure requirements;
- Clarify the definition of health care operations to excludes certain promotional communications; and
- Expand the Business Associates Agreement Requirements.

These and other developments make it imperative HIPAA covered entities and their business associates take prompt action to immediately review and update their data security and privacy practices to guard against growing liability exposures under HIPAA and other federal and state laws. Covered entities must update policies and practices to avoid these growing liabilities. Business associates that have not already done so also must appoint privacy officers and adopt and implement privacy and data security policies and procedures fully compliant with HIPAA and other applicable federal and state rules, including amendments enacted as part of the American Recovery and Reinvestment Act of 2009 signed into law on February 17, 2009.

For more information about today's announcement, go here. See here for the initial guidance and request for comments issued by HHS regarding these new security standards.

For More Information

We hope that this information is useful to you. If you need assistance with health care privacy and data security, technology, or other health care compliance, risk management, transaction or operation concerns, please contact the author of this update, Curran Tomko Tarski LLP Health Practice Group Chair, Cynthia Marcotte Stamer, at (214) 270-2402, cstamer@cttlegal.com or your other favorite Curran Tomko Tarski LLP Partner. Ms. Stamer has extensive experience advising clients and writes and speaks extensively on these and other health care privacy and data security and related matters.

You can review other recent health care and internal controls resources and additional information about the health industry and other experience of Ms. Stamer here. If you or someone else you know would like to receive future updates about developments on these and other concerns, please be sure that we have your current contact information – including your preferred e-mail – by creating or updating your profile at here or e-mailing this information to cstamer@cttlegal.com.