HHS and FTC Issue Guidance on Protection of Health Information

2009-05-06

The Department of Health and Human Services (HHS) and Federal Trade Commission (FTC) have issued guidance, proposed rules, and requests for information and public comments as they begin to implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was part of the American Recovery and Reinvestment Act economic stimulus legislation that President Obama signed on February 17, 2009.

The HITECH Act

As discussed in our February 24, 2009 alert, the HITECH Act directs HHS to issue regulations to, among other things, require HIPAA-regulated covered entities and their business associates to notify individuals whose health information is compromised in the event of a security breach involving unsecured protected health information. "Unsecured protected health information" is HIPAA-protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable through the use of a technology or methodology specified by HHS. The Act requires HHS to issue guidance specifying what technologies and methodologies are sufficient to make PHI secure.

The HITECH Act also recognizes that there are emerging web-based entities that are not covered entities under the existing HIPAA regulations, even though they exist to collect and maintain health information in personal health records (PHRs). PHRs contain PHI provided by or on behalf of the individual, and are managed, shared, and controlled by the individual. The Act requires HHS, in consultation with the FTC, to study potential privacy, security, and breach notification requirements for PHRs and make recommendations to Congress by February 2010 with respect to "vendors of personal health records," related entities, and third party service providers used by PHR vendors. Until Congress enacts new legislation implementing any recommendations contained in the report issued by HHS and the FTC, the HITECH Act imposes temporary PHR breach notification requirements to be enforced by the FTC.

HHS

On April 17, HHS issued guidance regarding the technologies and methodologies that can be used

to render PHI unusable, unreadable, or indecipherable to unauthorized individuals, thereby providing covered entities and their business associates with an optional safe harbor from application of the new data security breach notification requirement. HHS also requested public comments on this guidance and on the breach notification provisions of the HITECH Act, in order to inform future rulemaking.

The HHS guidance contains a list of methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. These methods fall into two categories: encryption and destruction.

- With regard to encryption, HHS views PHI as secure if it is encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such process or key has not been breached." The guidance identifies two encryption processes tested by the National Institute of Standards and Technology (NIST) judged to meet that standard—one for stored, or "at rest," data and another for transmitted data, or data "in motion."
- With regard to destruction, the guidance specifies that hard copy media such as paper and film must be shredded or destroyed so that the PHI cannot be read or reconstructed and that electronic media must be cleared, purged, or destroyed consistent with NIST-approved standards.

In addition to this guidance, HHS also solicited comment on two issues: (1) whether additional security technologies and methodologies should be added to the list in future iterations of the guidance; and (2) whether PHI in a "limited data set" lacking certain direct identifying fields should be treated as unusable, unreadable, or indecipherable to unauthorized individuals for purposes of the breach notification obligation.

Finally, HHS began the process of formulating breach notification regulations by soliciting public comments on a variety of questions focused primarily on identifying potential areas of conflict with existing state data security breach notification laws.

Comments and responses on the HHS guidance and notice must be submitted on or before May 21, 2009.

FTC

For the many PHR vendors that are not covered entities under HIPAA, the FTC issued a proposed rule on April 16, implementing the breach notification requirements applicable to vendors of PHRs, related entities, and third-party service providers of PHR vendors. The FTC provided examples of the types of entities covered by its proposed rules, including web-based applications that help consumers manage medications, websites offering a personalized health checklist, and brick-and-mortar companies advertising dietary supplements online. The FTC rule would also cover online applications that allow individuals to connect blood pressure cuffs, blood glucose monitors, or other devices to online applications and online medication or weight tracking programs that pull information from a personal health record. The FTC estimates that 200 vendors of personal health

records and 500 related entities will be covered by its proposed rule. Notably, the FTC's proposed rule applies to non-profit vendors, related entities, and third-party service providers that are otherwise outside of the FTC's traditional FTC Act jurisdiction to guard against unfair and deceptive commercial practices. The proposed rule applies only to entities that are not covered entities or business associates for purposes of HIPAA; those entities remain under the jurisdiction of HHS for purposes of breach notification obligations.

The FTC's proposed rule and notice provides guidance on what constitutes a "breach" triggering notification duties, noting that the rule creates a presumption that unauthorized persons have acquired information if they have access to it, but that such presumption can be rebutted with reliable evidence showing that the information was not or could not reasonably have been acquired. The proposed rule also provides detail on how and when to issue data security breach notifications to customers, the media, and the FTC, as well as the required contents of any notification.

In issuing its proposed rule, the FTC specifically sought comment on five issues: (1) the entities to which the proposed rule should apply; (2) the products and services they offer; (3) the extent to which vendors, related entities, and service providers might be HIPAA-covered entities; (4) whether some vendors of personal health records may have a dual role as business associates under HIPAA or direct providers of personal health records under HIPAA; and (5) circumstances in which such a dual rule might lead to consumers' receiving multiple breach notices. Comments on the FTC's notice are due on or before June 1, 2009.

These recent developments begin to explain and clarify how the Government will administer the HITECH Act requirements. The standards and practices adopted by the Government in implementing the HITECH Act are likely to become widely accepted industry expectations.

Authors

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089