

HHS and FTC Issue Guidance Regarding the Health Data Breach Notification Provisions and Invite Comment

By: Susan E. Gindin¹

On February 17, 2009, President Obama signed the stimulus package (the American Recovery and Reinvestment Act of 2009 (the "Recovery Act")) into law. Among other provisions of the massive law, the Recovery Act contains \$19 billion in incentives for advancement of a nationwide health information infrastructure and adoption of electronic medical records, along with far-reaching changes to HIPAA's privacy and security provisions.

Among the most significant changes made to HIPAA, the Recovery Act creates the first federal data breach notification statute. It applies to HIPAA covered entities and business associates, and also to vendors of personal health records ("PHR"), PHR related entities, and third party service providers (referred to in this article collectively as "PHR Handlers"). It also gives compliance oversight responsibilities to the Federal Trade Commission ("FTC") as well as the Department of Health & Human Services ("HHS").

In April, the HHS issued information security guidance and the FTC issued proposed regulations regarding the health data breach notification requirements, and each requests public comment. Interested parties have a short window of opportunity to provide comments and to influence the data breach notification rulemaking. The FTC's *Notice of Proposed Rulemaking* (the "FTC Proposed Rule"), which directly affects approximately 900 entities which are PHR vendors and related entities, and which have previously not been subject to HIPAA, requests public comment by June 1. The HHS *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements* ("HHS Guidance"), which will give compliant parties a safe harbor from the data breach reporting requirements, requests public comment by May 21. The HHS Guidance is of interest to a much larger group—the 900 PHR Handlers as well as HIPAA covered entities and business associates. In addition, because the Recovery Act is effectively the first federal data breach statute, the HHS Guidance is likely to become the standard of care going forward for all data breach notification statutes. Therefore, non-health care entities which own, license, or maintain personal information may also want to comment on certain parts of the HHS Guidance.

Background

Data breaches involving sensitive personal information may result in identity theft and financial crimes, and the FTC estimates that as many as 9 million Americans have their identities stolen each year. As noted, along with the push to adopt electronic health records, the Recovery Act tightens the HIPAA privacy and security rules by adding notification requirements in the event of a breach involving personal health information ("PHI").

¹ Copyright ©2009 Susan E. Gindin. Susan Gindin is Of Counsel to Isaacson Rosenbaum P.C. where she specializes in the areas of data privacy and security, advertising, new media, information technology and intellectual property law. Susan has been practicing in the area of data privacy and security law for more than thirteen years, and has been providing HIPAA guidance since 2002.

HHS and FTC Issue Guidance

Page 2

To give affected individuals notice that their PHI may have been accessed by unauthorized parties (and therefore an opportunity to try to prevent or minimize identity theft), the Recovery Act requires that covered entities, business associates, and PHR Handlers provide notice for breach of PHI data in any format--paper as well as electronic. The notification requirements are very exacting (for more detail, see Susan E. Gindin's *Understanding The Stimulus Package's Changes To HIPAA's Privacy Provisions* at <http://www.ir-law.com/5FBFD1/assets/files/lawarticles/UNDERSTANDING%20THE%20STIMULUS%20PACKAGE1.pdf>).

However, the Recovery Act also provides a compliance safe harbor if the data which is breached is in a "secure" format. Notification is required only for unsecured PHI which is defined as PHI that is not secured through a technology or methodology that HHS states renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals. The Recovery Act requires that HHS and FTC issue interim final regulations implementing the security breach notification requirements within 180 days of the Recovery Act's enactment, with the requirements becoming effective 30 days after the publication of such regulations (in September 2009).

The documents that were issued by HHS and FTC are steps towards implementation of the interim final regulations. The significant points and requests for comment include the following:

HHS Guidance

The HHS Guidance specifies two methods for securing PHI by rendering it unusable, unreadable or indecipherable: 1) encryption (as long as the encryption key has not been compromised) and 2) destruction. For destruction of media on which PHI is stored or recorded, paper, film or other hard copy must be shredded or destroyed so that it cannot be reconstructed, and electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization* (www.csrc.nist.gov) so that the PHI cannot be retrieved. Although only two methods are specified, the HHS Guidance also requests comments regarding whether there are additional methods for rendering PHI unusable, unreadable or indecipherable.

The HHS Guidance also notes that while adhering to the standards set forth in the Guidance gives affected entities a safe harbor from the notification requirements, affected entities must also follow all other applicable requirements, such as the HIPAA Privacy Rule's mitigation requirements and the state breach notification laws.

The HHS Guidance also requests comments regarding whether PHI in limited data set form should be treated as unusable, unreadable, or indecipherable to unauthorized individuals for purposes of breach notification.

Further, and of possible interest to handlers of personal information outside the health care industry as well as those covered by HIPAA, the HHS Guidance requests comments based on experience in complying with state breach notification laws, whether there any potential areas of conflict or other issues HHS should consider in promulgating the federal breach notification requirements; whether affected parties anticipate having to send multiple notices to an individual upon discovery of a single breach; whether there are circumstances in which the required federal notice would not also satisfy any notice obligations under the state laws; and whether entities exempt from notification under the HHS safe harbor may still need to notify individuals of a breach under state laws.

Finally, the Recovery Act defines "breach" as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." This concept that the unauthorized recipient could not retain the data codifies the fact that some technical "breaches" do not result in potential harm, and therefore are not required (or appropriate) to be reported. The definition goes on to provide several exceptions to the definition of breach where there was good faith acquisition, access or use by an employee or agent and there is no

HHS and FTC Issue Guidance

Page 3

further acquisition, access, use or disclosure, where there was inadvertent disclosure by an authorized agent to another at the same facility, or where PHI is not further acquired or disclosed.

The HHS Guidance notes these exceptions, and asks for public comment regarding “what particular types of circumstances entities anticipate these exceptions applying.”

FTC Proposed Rule

As noted, the Recovery Act requires that HIPAA covered entities, business associates, and PHR Handlers notify U.S. citizens and residents if their PHR is breached. Such entities are also required to notify the HHS, the FTC, and the media in certain circumstances. With regard to PHR Handlers, the Recovery Act directs the FTC to issue "temporary" regulations requiring such notifications.

The regulations are temporary in the sense that the Recovery Act requires HHS and FTC to study the potential privacy, security, and breach notification requirements related to such PHR Handlers and submit a report to Congress containing recommendations by February 17, 2010. These temporary security breach notification regulations will remain in place until Congress enacts new legislation.

The FTC notes that the Proposed Rule applies to these PHR Handlers regardless of whether such entities fall within the FTC's enforcement jurisdiction.

The FTC is seeking comment on a variety of issues within the Proposed Rule, including (1) the nature of entities to which the Proposed Rule would apply; (2) the particular products and services they offer; (3) the extent to which PHR Handlers may be HIPAA-covered entities or business associates of HIPAA-covered entities; (4) whether some PHR vendors may have a dual role as a business associate of a HIPAA-covered entity and a direct provider of PHR to the public; (5) circumstances in which such a dual role might lead to consumers receiving multiple breach notices or receiving breach notices from an unexpected entity, and whether and how the rule should address such circumstances; (6) whether spam filters will block email notices; (7) the standards that should apply to substitute media notice; and (8) questions in connection with the Paperwork Reduction Act and the Regulatory Flexibility Act.

Opportunity for Input

Data breaches can be extraordinarily expensive for affected individuals and organizations (the Ponemon Institute recently estimated that it costs organizations an average of \$6.6 million when an organization suffers a data breach). Data breach notifications are also expensive and time-consuming for affected organizations, and at the same time, a data breach notification can unduly alarm individuals when there has actually been no potential for identity theft. Now is the time for interested parties to provide their input for ensuring that information security guidelines and health data breach notification requirements are drafted appropriately so that personal health information is safeguarded, and so that individuals receive timely notice of data breaches but only when there is a potential for identity theft.

If you have any questions about the HHS Guidance, FTC Proposed Rule, or any other information privacy or security issues, please contact Susan Gindin at 303-256-7046 or sgindin@ir-law.com.