Compliance Advisory:

Health Breach Notification Rule

MEADE & ROACH LLP

May 2009

FTC Published Proposed Rule Addressing Security Breach Notification Obligations of Personal Health Record Vendors

On April 20, 2009, the Federal Trade Commission ("FTC") published a notice of proposed rulemaking. The proposed rule (the "Proposed Rule"), which is required by the HITECH provisions of the American Recovery and Reinvestment Act of 2009 (the "Act"), addresses notice obligations of vendors of personal health records ("PHRs") following a breach of security of unsecured PHR identifiable health information. 74 Fed. Reg. 17914 (April 20, 2009). The Proposed Rule does not apply to HIPAA-covered entities; however, the Proposed Rule provides significant guidance and insight as to what the Department of Health and Human Services ("HHS") may propose once it publishes its notification rule governing security breaches of protected health information maintained by HIPAA-covered entities and their business associates.

> "The Proposed Rule changes the regulatory landscape and PHR vendors should waste no time in assembling the infrastructure necessary to ensure compliance."

Key Definitions (16 C.F.R. § 318.2)

The Proposed Rule addresses a number of key definitions, including:

1. Breach of Security: The FTC acknowledges that a person's unauthorized access to unsecured PHR identifiable health information may not result in the improper acquisition of such information. However, the Proposed Rule creates a rebuttable presumption that if a person obtains unauthorized access to unsecured PHR identifiable information then they have acquired that information.

> This is a critical operational issue for PHR vendors. As part of their security breach notification policies and procedures, PHR vendors should incorporate a process to ascertain whether it is possible to rebut the presumption of acquisition. The FTC provides examples of evidence that could rebut this presumption, including a forensic analysis to establish that files on a recovered laptop were never opened, altered, transferred or otherwise compromised.

2. PHR Identifiable Health Information: Drawing from the plain language of the Act, the FTC would broadly define the term "PHR identifiable health information" to include individually identifiable health information under HIPAA that is provided by or on behalf of the individual and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. Based upon that proposed broad definition, the FTC notes that: (1) a security breach of unsecured PHR identifiable health information could include a breach of a database containing only names and credit card information; (2) a security breach requiring notification could involve a breach of the mere fact that a person has an account with a vendor of PHR for persons with a particular health condition (e.g., HIV or AIDS); and (3) if there is no reasonable basis to believe that improperly accessed and acquired information can be used to identify an individual (e.g., the information has been de-identified), then the information is not

PHR identifiable health information and notice of a security breach involving that information is not required.

3. PHR Related Entity. The FTC makes it clear that a "PHR related entity" is not a HIPAA-covered entity. However, an entity could be both a PHR related entity, subject to governance and enforcement by the FTC, and a HIPAA-covered entity, subject to governance and enforcement by HHS.

4. Unsecured. The FTC specifically defines "unsecured" to mean not protected through the use of a technology or methodology specified by HHS in the guidance issued under the Act. For additional information about the guidance issued by HHS regarding the security of protected health information, see our Client Advisory dated April 2009 (http://meaderoach.com/Resource/Compliance%20Advisory%20-%20Unsecured%20PHI.pdf).

PHR vendors should carefully consider whether they can encrypt or otherwise secure PHR identifiable health information, as the notice obligations set forth in the Proposed Rule apply only to breaches of unsecured PHR identifiable health information.

Breach Notification Obligation (16 C.F.R. § 318.3)

There are several key components to the FTC's proposed breach notification obligation:

1. Third party service providers are obligated to: (a) notify a "senior official" of the vendor of PHRs or PHR related entity of a security breach; and (b) obtain acknowledgement from such official that she received the notification.

Vendors of PHR and their third party service providers should consider whether these obligations should be specifically incorporated into their operative service agreement.

2. The Proposed Rule specifies that the breach will be deemed to have been discovered on the first day on which the breach is known or should reasonably have been known to such vendor of PHRs.

The "reasonably should have been known standard" will require PHR vendors to implement policies, procedures and practices to promptly detect security incidents. Thus, employees and vendors of PHR vendors will need to be properly trained to investigate, discover and report security incidents.

Timeliness of Notification (16 C.F.R. § 318.4)

The Proposed Rule would require breach notifications to individuals and the media to be made "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach. Thus, the burden is on the PHR vendor to report security breaches to consumers as soon as practicable and the FTC notes specifically that "in some cases, it may be an 'unreasonable delay' to wait until the 60th day" to provide notification.

PHR vendors should establish policies and procedures to address the investigation and response to security incidents. Responsible parties and duties should be clearly identified. Waiting until such time as there is a security incident involving PHR identifiable health information to implement such policies and procedures may cause the PHR vendor to violate its prompt notice obligation.

Methods of Notice (16 C.F.R. § 318.5)

The Proposed Rule addresses notice to individuals, the FTC and the media.

1. Individual Notice: Considerable discussion is paid to the appropriate methods of notice for individuals.

   a. Notice by First Class Mail or E-mail. The Proposed Rule specifies that individuals must be given notice of a security breach by first-class mail or, if the individual provides "express affirmative consent," by e-mail. Although the default notice mechanism is first-class mail, the FTC acknowledges that e-mail notice may be particularly well-suited to the relationship between a PHR vendor and consumer.

   b. Telephonic Notice. The Proposed Rule also

provides for telephonic notice or notice by "other appropriate means," in addition to first-class mail or e-mail notice, if there is possible imminent misuse of unsecured PHR identifiable information.

c. Substitute Notice. Finally, the Proposed Rule provides for the provision of a substitute form of actual notice if the individual's preferred method of communication is determined to be insufficient (e.g., first-class or e-mail notice is returned as non-deliverable). The Proposed Rule specifies that if ten (10) or more customers cannot be reached, the PHR vendor must provide substitute notice in one of two forms: (a) through the home page of its website; or (b) through major print or broadcast media. In either case, the PHR vendor must include a toll-free phone number where an individual can learn whether his/her unsecured PHR identifiable health information may have been breached. In doing so, however, the FTC cautions that the vendor should have reasonable procedures in place to verify that they are providing the requested information only to the individual and not to an unauthorized person.

With respect to substitute notice via the PHR vendor's website, the Proposed Rule specifies that the notice must be "conspicuous" and remain on the website for at least 6-months. To be conspicuous, a hyperlink to the beach notice must be prominent so that it is noticeable to consumers and worded to convey the nature and importance of the information to which it leads. The FTC states specifically that "click here" is likely not conspicuous, but "click here for an important notice about a security breach that may affect you" would be. The FTC also observes that posting on the PHR vendor's home page should take into account the home page for both new visitors and existing account holders (i.e., existing account holders may be directed to a different home page than new visitors). The FTC concludes that because PHRs generally involve an online relationship, web posting would be a particularly well-suited method of substitute notice to individuals.

If substitute notice is to be provided via a media outlet, the Proposed Rule would require such notice to be "reasonably calculated to reach the individuals affected." Further, a media notice can only be reasonably calculated to reach the individuals affected if it is "clear and conspicuous." Thus, the notice should be stated in plain language, be prominent, and run multiple times.

2. Media Notice. If a security breach involves unsecured PHR identifiable health information of 500 or more residents of a given state or jurisdiction, the Act and the Proposed Rule would require media notice. This media notice is different than the substitute media notice for individual notice described above in that it is notice direct "to" the media (as opposed to notice directed to individuals that is disseminated via the media) and is intended to supplement and not substitute for the requisite individual notice. In other words, if a breach involves 500 or more residents in a given state or jurisdiction, then both individual (or substitute) and media notice are required.

According to the Proposed Rule, the required media notice should include the dissemination of a press release.

3. Notice to the FTC. If a breach involves the unsecured PHR identifiable health information of 500 or more individuals then the PHR vendor must notify the FTC as soon as possible and in no case later than five (5) business days after discovery of the breach. If a breach involves fewer than 500 individuals, then the PHR vendor may, in lieu of immediate notice, maintain a breach log to be submitted on an annual basis to the FTC. The first log is to be submitted no later than one-year from the date of the PHR vendor's first security breach. The FTC expects to publish a form of notice log that may be used by PHR vendors.

Content of Notice to Individuals (16 C.F.R. § 318.6)

The Proposed Rule would require a security breach notice to individuals to include:

- a description of how the breach occurred;
- a description of the types of unsecured PHR

identifiable health information that were involved in the breach;
- the steps individuals should take to protect themselves from potential harm;
- a description of what the PHR vendor is doing to investigate the breach, to mitigate any losses and to protect against any further breaches; and
- contact procedures for individuals to ask questions or learn additional information.

The FTC states specifically that notices should NOT include any personal or financial information.

Historically, PHR vendors have not been subject to much regulatory oversight at the federal level. The Proposed Rule changes the regulatory landscape that PHR vendors have been subject to, and PHR vendors should waste no time in assembling the infrastructure necessary to ensure compliance.

Although the Proposed Rule is only applicable to PHR vendors and PHR related entities and not to HIPAA-covered entities, covered entities should also carefully review the rule as a possible precursor to a companion rule to be published by HHS.

If you have any questions, please contact:

Brian D. Annulis at 312.218.7258 or BAnnulis@MeadeRoach.com

Ryan D. Meade at 312.498.7004 or RMeade@MeadeRoach.com

Steven W. Ortquist at 312.285.4850 or SOrtquist@MeadeRoach.com

Michael C. Roach at 312.255.1773 or MRoach@MeadeRoach.com