

Health Care ADVISORY

April 20, 2009

PHR Vendors and Related Entities Face The FTC'S New Health Breach Notification Rule

On April 16, the Federal Trade Commission (FTC) issued a Notice of Proposed Rulemaking (the "Proposed Rule" or the "Health Breach Notification Rule") requiring vendors of personal health records (PHR) and related entities to notify individuals when the security of their individually identifiable health information is breached.¹ The Proposed Rule establishes a new Part 318 of Title 16 of the Code of Federal Regulations for the health breach notification requirement that was mandated by Section 13407 of the American Recovery and Reinvestment Act of 2009 (ARRA).² The FTC is accepting comments on the Proposed Rule through June 1, 2009, after which the FTC will issue an interim final rule in early August as required under ARRA.

The new Health Breach Notification Rule would require web-based entities that have access to an individual's PHR, and are not covered entities or business associates under the Health Insurance Portability and Accountability Act (HIPAA), to notify such individuals in the event that their PHR has been breached. As discussed in the Proposed Rule, this new requirement runs parallel to the breach notification requirement that will apply to covered entities and business associates, which will be promulgated in forthcoming rulemaking from the Department of Health and Human Services (HHS), as required by ARRA.

In general, the Proposed Rule is substantively similar to the provisions of Section 13407 of ARRA. The FTC is using this opportunity, however, to shed additional light on certain definitions and aspects of the Health Breach Notification Rule. This advisory highlights the key provisions of the Proposed Rule, including those sections where the FTC is seeking public comment.

What Is PHR?

As defined in ARRA, PHR is an "electronic record of 'PHR identifiable health information' on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." The term "PHR identifiable health information" is defined as "individually

¹ See 74 *Fed. Reg.* 17914 (April 20, 2009) available at <http://edocket.access.gpo.gov/2009/pdf/E9-8882.pdf>.

² American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

identifiable health information”³ (as defined in the Social Security Act) and, with respect to an individual, information (1) that is provided by or on behalf of the individual; and (2) 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. It is important to note that, if there is no reasonable basis to believe that the information can be used to identify the individual, the information is not “PHR identifiable health information” and, thus, notification of a breach is not required.

Who Must Comply with the Health Breach Notification Rule?

The Health Breach Notification Rule is intended to reach entities that are neither covered entities nor business associates, as defined under HIPAA. The Proposed Rule would apply to vendors of PHR, PHR related entities and third party service providers. Specifically, the goal of the Proposed Rule is to reach web-based entities that collect consumers’ health information, such as vendors of PHR and online applications that interact with such PHR. The FTC notes that the Proposed Rule applies to these entities regardless of whether such entities fall within the FTC’s enforcement jurisdiction. The Proposed Rule defines these entities as follows:

- **PHR Vendors** are entities (other than HIPAA-covered entities or entities that act on behalf of HIPAA-covered entities as business associates) that offer or maintain a PHR.
- **PHR Related Entities** are entities (other than HIPAA-covered entities or entities that act on behalf of HIPAA-covered entities as business associates) that do any of the following:
 - offer products or services through the website of a vendor of PHR (e.g., a web-based application that helps consumers manage medications);
 - offer products or services through the websites of HIPAA-covered entities that offer individuals’ PHR; or
 - access information in a PHR or send information to a PHR (e.g., online applications through which individuals can connect their blood pressure cuffs or other devices, so that the results could be tracked through their PHR).
- **Third Party Service Providers** are entities that (1) provide services to a vendor of PHR in connection with the offering or maintenance of a PHR, or to a PHR related entity in connection with a product or service offered by that entity; and (2) access, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose unsecured PHR identifiable health information as a result of such services. An example of a third party service provider is an entity that provides billing or data storage services to vendors of PHR or PHR related entities.

³ Section 1171(6) of the Social Security Act (codified at 42 U.S.C. § 1320d(6)) defines “individually identifiable health information” as any information that (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual.

The FTC is seeking comment on the following: (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 vendors of PHR, PHR related entities and third party service providers may be HIPAA-covered entities or business associates of HIPAA-covered entities; (4) whether some vendors of PHR may have a dual role as a business associate of a HIPAA-covered entity and a direct provider of a PHR to the public; and (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.

How Is a Breach of Security Defined?

As in ARRA, the Proposed Rule defines a breach of security as the *acquisition*⁴ of unsecured⁵ PHR identifiable health information of an individual in a PHR without the authorization of the individual. The Proposed Rule, however, would add to the definition that “[u]nauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of [PHR], PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition of such information.”

Accordingly, the Proposed Rule creates a presumption that unauthorized persons have acquired information if they have access to it, thereby creating the obligation to provide breach notification. However, this presumption can be rebutted with reliable evidence demonstrating that the information was not or could not reasonably have been acquired. The FTC offers the example of an employee losing his or her laptop containing unsecured health information in a public place. The FTC states that, because the information would be accessible to unauthorized persons, there would be the presumption that an unauthorized acquisition has occurred. The entity, however, could rebut this presumption by demonstrating that the laptop was recovered and that forensic analysis revealed that the files were never opened, altered, transferred or otherwise compromised.

What Are the Breach Notification Requirements?

In general, the Proposed Rule would require that, following the discovery of a breach of security of unsecured PHR that is held in a PHR either maintained or offered by a vendor of PHR, such vendor and each PHR related entity notify each individual whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of the breach and the FTC. A third party service provider would be required to notify the PHR vendor or PHR related entity upon discovery of such

⁴ The FTC suggests that the information must not only be available to unauthorized persons, but actually *obtained* by unauthorized persons.

⁵ The term “unsecured” means PHR identifiable information that is not protected through the use of technology or methodology specified by the Secretary of HHS. On April 17, 2009, the Secretary issued guidance specifying such technologies and methodologies to render protected health information (PHI) unusable, unreadable or indecipherable to unauthorized individuals, as required by ARRA. See <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf>.

breach. The Proposed Rule makes clear that the third party service provider would be required to notify a senior official of the PHR vendor or PHR related entity, and obtain acknowledgment that the notification has been received to ensure that the message is appropriately relayed.

A breach would be treated as discovered as of the first day on which the breach is *known* to the PHR vendor, PHR related entity or third party service provider (including any person, other than the individual committing the breach, that is an employee, officer or other agent of such PHR vendor, PHR related entity or third party service provider), or reasonably should have been known to have occurred. The FTC provides that the “reasonably should have been known” standard requires the entity to maintain reasonable security measures (e.g., breach detection measures) to ensure that breaches are discovered in a timely manner.

Notice to the Individual

All notifications of a breach to individuals would be required to be made without unreasonable delay and not later than 60 calendar days after discovering the breach, unless such notification would impede a criminal investigation or harm national security. If 10 or more individuals cannot be reached by written notice or the individual’s preferred form of communication (e.g., electronic mail), the PHR vendor or PHR related entity would be required to provide notice through a conspicuous posting on its home page or in major print or broadcast media. The FTC is seeking comments on the standards that should apply to substitute media notice.

Notice to the Media

A PHR vendor or PHR related entity would be required to provide notice to prominent media outlets serving the state or jurisdiction following the discovery of a breach of security, if the breach involves unsecured PHR identifiable health information of 500 or more residents of that state or jurisdiction. The FTC observes that this notification of the media where more than 500 individuals are involved is intended to supplement and not replace the substitute media notice intended for individuals that cannot be reached after making other reasonable efforts. The FTC is requesting comments on the standards and criteria that should apply in determining the adequacy of such media notice.

Notice to the FTC

Similar to the notice of the media provision, a PHR vendor or PHR related entity would be required to notify the FTC as soon as possible, and in no case later than five business days, if the breach of unsecured PHR identifiable health information involves 500 or more individuals. If the breach involves less than 500 individuals, PHR vendors and PHR related entities may, instead, maintain a log of the breaches and submit the log annually to the FTC. According to the Proposed Rule, the FTC intends to develop a form to be used by entities for both immediate and annual notices that will be posted on its website.

What Should Be Included in the Notice to Individuals?

The FTC makes clear the content of the notices for individuals. Specifically, notification to individuals should include the following: (1) a description of the types of unsecured PHR identifiable health information that were involved in the breach; (2) the steps individuals should take to protect themselves from potential harm; (3) a description of what the vendor of PHR or PHR related entity involved is doing to investigate the breach, to mitigate any losses and to prevent any further breaches; and (4) contact procedures for individuals to ask questions or learn additional information. Addressing the element of providing individuals with steps to protect themselves in the future, the FTC makes a few suggestions. If an individual's health insurance account information is compromised, for example, the FTC suggests that the PHR vendor or PHR related entity could encourage the individual to request and review copies of their medical files for potential errors, or monitor explanation of benefit forms for potential errors.

How Will the Health Breach Notification Rule Impact PHR Vendors and PHR-Related Entities Financially?

The FTC estimates that approximately 900 entities will be subject to the breach notification requirements in the Proposed Rule. This includes 200 vendors of PHR, 500 PHR related entities and 200 third party service providers. The agency also estimates that each entity will experience 11 breaches per year that may require notification. To determine the financial cost to each entity, the FTC estimated the costs associated with the following three categories: (1) the costs of determining which information has been breached, identifying customers who are affected by the breach, preparing the breach notice and reporting the breach to the FTC; (2) the costs associated with notifying affected consumers; and (3) the costs involved with setting up a toll-free number, if needed. In total, the FTC estimates the annual cost burden associated with the breach notification requirements for each entity will equal \$1,020,625. The FTC is seeking comments with respect to the financial cost estimates of the breach notification requirement.

What Is the Relationship of the Health Breach Notification Rule to HIPAA and Other Laws?

According to the FTC, there are no federal statutes, rules or policies currently in effect that would conflict with the Proposed Rule. However, because there is the potential that the forthcoming HHS regulations governing breach notification for covered entities and business associates will overlap with the FTC's requirement, the FTC is consulting with HHS on this matter. The FTC is requesting comments on this potential overlap, as well as any other potentially duplicative, overlapping or conflicting federal statutes, rules or policies.

If you would like to receive future *Health Care Advisories* electronically, please forward your contact information including e-mail address to healthcare.advisory@alston.com. Be sure to put “**subscribe**” in the subject line.

For further guidance on HIPAA security or privacy compliance relating to the changes implemented by ARRA, please contact one of the attorneys or advisors listed below:

Washington Office

Jacqueline C. Baratian
202.756.3484
jacqueline.baratian@alston.com

Jennifer L. Butler
202.756.3326
jennifer.butler@alston.com

Elinor A. Hiller
202.756.3401
elinor.hiller@alston.com

Laura E. Holland
202.239.3980
laura.holland@alston.com

Peter M. Kazon
202.756.3334
peter.kazon@alston.com

Stephanie A. Kennan
Senior Public Policy Advisor
202.756.3159
stephanie.kennan@alston.com

Keavney F. Klein
202.239.3981
keavney.klein@alston.com

Rudy S. Missmar
202.756.3034
rudy.missmar@alston.com

Mark Rayder
Senior Public Policy Advisor
202.756.3562
mark.rayder@alston.com

Colin T. Roskey
202.756.3436
colin.roskey@alston.com

Marc J. Scheineson
202.756.3465
marc.scheineson@alston.com

Thomas A. Scully
202.756.3459
thomas.scully@alston.com

Donald E. Segal
202.756.3449
donald.segal@alston.com

Tamara R. Tenney
202.756.3489
tamara.tenney@alston.com

Julie K. Tibbets
202.756.3444
julie.tibbets@alston.com

Timothy P. Trysla
202.756.3420
tim.trysla@alston.com

Tiffani V. Williams
202.756.3412
tiffani.williams@alston.com

Marilyn Yager
Senior Public Policy Advisor
202.756.3341
marilyn.yager@alston.com

Atlanta Office

Donna P. Bergeson
404.881.7278
donna.bergeson@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Jeffrey K. Hester
404.881.4254
jeff.hester@alston.com

Robert C. Lower
404.881.7455
bob.lower@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

D'Andrea J. Morning
404.881.7538
dandrea.morning@alston.com

Robert D. Stone
404.881.7270
robert.stone@alston.com

Michelle A. Williams
404.881.7594
michelle.williams@alston.com

ATLANTA

One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404.881.7000

CHARLOTTE

Bank of America Plaza
Suite 4000
101 South Tryon Street
Charlotte, NC 28280-4000
704.444.1000

DALLAS

Chase Tower
Suite 3601
2200 Ross Avenue
Dallas, TX 75201
214.922.3400

LOS ANGELES

333 South Hope Street
16th Floor
Los Angeles, CA 90071-3004
213.576.1000

NEW YORK

90 Park Avenue
New York, NY 10016-1387
212.210.9400

RESEARCH TRIANGLE

Suite 600
3201 Beechleaf Court
Raleigh, NC 27604-1062
919.862.2200

SILICON VALLEY

Two Palo Alto Square
Suite 400
3000 El Camino Real
Palo Alto, CA 94306-2112
650.838.2000

VENTURA COUNTY

Suite 215
2801 Townsgate Road
Westlake Village, CA 91361
805.497.9474

WASHINGTON, D.C.

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202.756.3300

www.alston.com

© Alston & Bird LLP 2009