

Client Alert

Latham & Watkins
Health Care Practice

Federal Trade Commission Data Breach Notification Rule Regarding Personal Health Records

Organizations with Web sites that allow people to maintain their medical information online or who provide applications for personal health records will need to read and comply with the Federal Trade Commission's Health Breach Notification Rule, issued on August 17, 2009. The Federal Trade Commission (FTC) estimates that 900 entities will be subject to these new breach requirements, including 200 vendors of Personal Health Records (PHRs), 500 PHR-related entities, and 200 third-party service providers.

The FTC's Final Rule requires vendors of personal health records and related entities to notify consumers in the event of a breach of their personal health information. This new rule has broad implications for non-HIPAA-covered entities and may require vendors and their related entities to alter their security breach identification and notification measures. The Department of Health and Human Services (HHS) issued a companion rule for entities covered by the Health Insurance Portability and Accountability Act (HIPAA), which is summarized in [Client Alert 929](#).

Background

The American Recovery and Reinvestment Act of 2009 (Recovery Act) aims to expand the use of electronic health record systems by medical professionals. Recognizing the privacy risks involved in this expansion, the Recovery Act includes provisions for protecting the privacy of online healthcare consumers. In particular, the Recovery Act requires HHS and FTC to study and recommend privacy and security measures for Congress to enact. Until Congress enacts these provisions, the Recovery Act requires vendors of public health information to notify consumers in the event of a security breach. FTC's new rule (16 CFR Part 318) implements this requirement for entities not covered by HIPAA.

Who Must Comply

The FTC's Health Breach Notification Rule applies broadly to non-HIPAA-covered entities who are vendors and custodians of PHR defined as electronic records of health information that can be identified with a particular individual. Even non-profit organizations, traditionally outside the scope of the FTC's jurisdiction, who sell or store

"Violation of this rule will be treated by the FTC as an unfair or deceptive act in violation of the Federal Trade Commission Act, and punished accordingly."

PHRs are subject to the rule, as are foreign vendors that maintain health information of US residents and citizens. The rule applies to three types of organizations:

- **PHR vendors**—entities, other than HIPAA-covered entities or business associates of a HIPAA-covered entity (when acting in such capacity), that offer or maintain a PHR (**including platforms such as Revolution Health, Google Health and Microsoft Health Vault and individual PHR vendors such as WebMD and ActiveHealth**).
- **PHR-related entities**—entities, other than HIPAA-covered entities or entities to the extent that they engage in activities as a business associate of a HIPAA-covered entity, that:
 - Offer products or services through the Web site of a PHR vendor (such as a Web-based application that helps consumers manage medications),
 - Offer products or services through the Web sites of HIPAA-covered entities that offer individuals PHRs, or
 - Access information in a PHR or send information to a PHR (such as online applications facilitating the connection of devices such as blood pressure cuffs, so that results are tracked through to a PHR).
- **Third-party service providers (TPSP)**—entities that:
 - Provide services to a PHR vendor 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 (such as billing or data storage companies), and
 - Access, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose unsecured PHR identifiable health information as a result of such services.

Entities covered by HIPAA are required to comply with the companion HHS rule, issued August 19, 2009 (and summarized

in a separate *Client Alert* for HIPAA-covered entities: [Client Alert 929](#).

Types of Information Subject to the Rule

The Recovery Act defined PHR as those records managed, shared and controlled by or primarily for the individual (and not the kinds of records managed by or for commercial enterprises, such as life insurance companies maintaining records for their own business purposes). The law includes electronic records of personal health information, regardless of whether they were created or received by a health care provider, health plan, employer or health care clearinghouse. "PHR identifiable health information" is information, including demographic information, that 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; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

As interpreted by the FTC, this requirement can be met with minimal information. For example, if the Web site caters to a particular type of customer (*e.g.*, cancer patients), then *the mere fact of* having an account with this vendor constitutes a PHR. Similarly, the disclosure of names or credit card information can trigger notification if this disclosure identifies an individual as a customer of a particular product or Web site associated with a particular health condition. Given the proliferation of such sites handling credit card information, this expansive definition could sweep a great number of entities into coverage under this regulation.

Importantly, the notification requirements apply only to health information that is not secured through technologies specified by HHS. This

means that if appropriately encrypted data is lost or stolen, a breach has not occurred for notification purposes. De-identified information also falls outside the rule.

Rebuttable Presumption that Access to Personal Health Records Means Acquisition of these Records

In its proposed rule, FTC recognized a distinction between unauthorized *access* to health information (*i.e.*, the opportunity to view PHRs) and unauthorized *acquisition* (*i.e.*, the actual viewing of PHRs). The proposed rule established a rebuttable presumption that access would imply acquisition. Thus, unauthorized access would require notification, unless the entity could show with reliable evidence that there had not been, or could not have been, unauthorized acquisition.

The FTC provided two useful examples of the interplay between access and acquisition. If, for example, a vendor's unauthorized employee accidentally logs on to a consumer's PHR, access has occurred. However, if the entity can show that the employee did not read the information available on his or her screen and instead promptly logged off, no acquisition has occurred, and notification would not be necessary.

Even more evocative is the example of an employee leaving a laptop in a public place. A lost laptop allows for access to the computer's information for anyone who finds it. However, if the entity can show that the employee located the laptop before anyone had an opportunity to open it and view its files, then acquisition did not occur, and the entity would not need to notify consumers.

When first proposed, this rebuttable presumption raised concerns among many commenters. Some argued that the rebuttable presumption renders the distinction between access and acquisition "hollow" because it is

too difficult to prove conclusively in a given circumstance that access did not lead to acquisition. Nevertheless, the FTC rejected alternatives, such as requiring an objectively reasonable expectation of harm from the access before notification would be necessary. The agency acknowledged that access does not always lead to acquisition, but concluded that the sanctity of personal health information means vendors should default toward notification when unauthorized access has occurred. The FTC expressed concern that vendors are not in a position to determine whether a consumer has been harmed by the disclosure of his/her health information, so determining likelihood of harm would be an unacceptably subjective task. Further, the FTC assumed that consumers want to know every time their health information may have been breached, regardless of the likely harm resulting from the breach. For these reasons, FTC included the rebuttable presumption in the final rule.

Rule Requires Vigilance In the Detection of Breaches and Swift Action in the Event of a Breach

The rule requires permanent vigilance on the part of vendors, PHR-related entities and TPSP. Though the rule does not establish a security standard, it does expect entities to perform breach-detection measures. Whether or not an entity maintained such measures will factor into the FTC's determination of whether an entity reasonably should have discovered a breach. Thus, failure to use such measures could result in violation of the rule.

Discovery by vendors and PHR-related entities

If a vendor or PHR-related entity discovers a breach, it must notify all US consumers whose information was acquired by an unauthorized person. Notification must be made by first-class

mail, unless the consumer has indicated a preference for notification by e-mail.

Notice must include:

- an explanation of the breach,
- a description of the information likely acquired,
- steps individuals can take to protect themselves from harm resulting from the breach,
- an explanation of what the entity is doing to investigate the breach, mitigate harm and protect against further breaches, and
- contact information customers can use to ask questions or learn more.

Vendors and PHR-related entities must notify consumers promptly, without "unreasonable delay," and in no case more than 60 calendar days after discovery of the breach.

In addition, vendors and PHR-related entities must notify major media outlets in all states or jurisdictions in which 500 or more residents were compromised by the breach.

Likewise, vendors and PHR-related entities must notify the FTC within 10 days if a breach involved 500 or more consumers. If fewer consumers were involved in the breach, covered entities can wait to notify the FTC at the end of the calendar year. When reporting health breaches, FTC will require parties to complete and file a standard Notice of Breach of Health Information form, available here: <http://www.ftc.gov/os/2009/08/R911002hbnform.pdf>.

Discovery by Third-Party Service Providers

If a TPSP discovers a breach, it must notify the related vendor or PHR-related entity of the breach in a timely manner, in no case more than 60 days after

discovery of the breach. The clock then begins for the vendor or PHR-related entity to notify the affected consumers.

Interaction with State Laws

The rule's notification requirements preempt contrary state laws. State law is contrary to this rule if it would be impossible to comply with both the state law and the rule, or if the state law is an impediment to enforcement of the rule. If state law is consistent with this rule, then entities must comply with both.

Nearly all of the states have laws governing notification of customers in the event of a breach of security. Understanding whether a particular breach triggers inconsistent or parallel additional state law compliance steps will require companies to have a rapid response capability in terms of identifying the universe of impacted users, the triggered state laws and a compliant plan for notification.

Enforcement, Effective Date and Sunset of the Rule

Violation of this rule will be treated by the FTC as an unfair or deceptive act in violation of the Federal Trade Commission Act, and punished accordingly. The rule will take effect on September 24, 2009 and applies to breaches of security discovered on or after this date. The FTC will not begin enforcement until February 2010.

Application of this rule is expected to be temporary, as the Recovery Act commits Congress to enact legislation on health breach notification. Congress is currently awaiting recommendations by FTC and HHS and will then begin to enact federal legislation on this subject matter.

If you have any questions about this *Client Alert*, please contact one of the authors listed below or the Latham attorney with whom you normally consult:

Jennifer C. Archie
+1.202.637.2205
jennifer.archie@lw.com
Washington, D.C.

Kevin C. Boyle
+1.202.637.2245
kevin.boyle@lw.com
Washington, D.C.

Micah Schwartz*
+1.202.637.2362
micah.schwartz@lw.com
Washington, D.C.

**Licensed to practice law in Virginia only; all work directly supervised by a member of the District of Columbia Bar.*

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the attorney whom you normally consult. A complete list of our *Client Alerts* can be found on our Web site at www.lw.com.

If you wish to update your contact details or customize the information you receive from Latham & Watkins, please visit www.lw.com/LathamMail.aspx to subscribe to our global client mailings program.

| | | |
|------------------|----------------------|-------------------------|
| Abu Dhabi | London | Paris |
| Barcelona | Los Angeles | Rome |
| Brussels | Madrid | San Diego |
| Chicago | Milan | San Francisco |
| Doha | Moscow | Shanghai |
| Dubai | Munich | Silicon Valley |
| Frankfurt | New Jersey | Singapore |
| Hamburg | New York | Tokyo |
| Hong Kong | Orange County | Washington, D.C. |