WSGR ALERT

SEPTEMBER 2009

NEW HEALTH SECURITY BREACH NOTIFICATION RULES BECOME EFFECTIVE

Interim final rules implementing security breach notification requirements for personal health data released by the Federal Trade Commission (FTC) and the Department of Health and Human Services (HHS) create new compliance obligations. The rules apply to certain entities governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations as well as entities that sell and/or maintain personal health records (PHR), and require that these entities notify affected individuals in the event that the security of their personal health information is breached. The American Recovery and Reinvestment Act of 2009 (ARRA) mandated the new regulations.[1] The FTC rule applies to security breaches that are discovered on or after September 24, 2009, while the HHS rule became effective on September 23, 2009.[2]

The FTC Rule: Vendors, PHR-Related Entities, Third Parties

The FTC rule requires that various entities[3] that maintain or offer personal health records provide specific notifications to individuals and to the FTC upon discovery of any security breach involving *unsecured*[4] PHR. Notification must be provided to affected individuals no later than 60 days after the entity knew, or should have known, that the breach occurred. If more than 500 individuals in any single state are affected, notice must also be given to prominent media outlets in that state. Further, if the breach involves the PHR of more than 500 individuals in total—regardless of where the affected persons are located—the FTC must be notified of the breach no later than 10 business days after discovery. If the breach affects less than 500 individuals, a log must be kept and provided to the FTC on an annual basis. Breach notifications required under the FTC rule must be made by specific methods and contain certain information.[5]

The HHS Rule: HIPAA-Covered Entities and Business Associates

The HHS breach notification rule governs security breaches involving information maintained by HIPAA-covered entities or business associates of HIPAA-covered entities. Business associates, in particular, will want to familiarize themselves with the new requirements. In some respects, both the FTC and HHS rules impose similar obligations. For example, like the FTC rule, the HHS rule only requires notification in the event of a breach involving *unsecured* data. Further, both rules require notice to affected individuals within 60 calendar days following discovery of the breach and, in the event that more than 500 individuals are affected, notice to the media.[6]

Differences in the HHS and FTC Rules

There are some differences in the two rules that could affect some organizations' efforts to comply. For example, unlike the FTC rule, the HHS rule allows 60 days for notification of the agency when a breach involves 500 or more affected individuals, regardless of the location of those 500 persons, rather than the 10-day notice period under the FTC rule.[7] Additionally, in some circumstances, an unauthorized disclosure of unsecured personal health information may not constitute a breach requiring notification under the HHS breach notification rule so long as the HIPAA-

---

[1] *See generally* "Health Privacy Changes Create Increased Risks and Obligations for Holders of Health Data," WSGR Client Alert, July 7, 2009.

[2] Both the FTC and HHS have exercised their discretion and allowed for a 180-day grace period before bringing enforcement actions for breaches discovered before February 22, 2010. Risks of parallel state enforcement efforts under a variety of laws and guidance from the agencies suggest the importance of complying during this interim period.

[3] The FTC requirements apply to: (1) vendors of personal health records, (2) PHR-related entities, and (3) third-party service providers. The FTC rule does not apply to HIPAA-covered entities or business associates of HIPAA-covered entities.

[4] Both the FTC and HHS incorporated the standard for how information may be secured set out in the HHS guidance issued April 17, 2009. Acceptable security measures include encryption and destruction such that the protected health information is unusable, unreadable, or indecipherable to unauthorized individuals.

[5] Notification must be provided by written notice sent via first-class mail to the last known address of the individual. However, if a reasonable effort is made to contact all affected individuals, and the notifying entity finds that contact information of 10 or more individuals is insufficient or out of date, then notice must be made through another form that it is reasonably calculated to reach the affected individuals. Substitute notice may consist of: (1) a conspicuous posting for a period of 90 days on the home page of the notifier's website; or (2) through major print or broadcast media. The notice must include a description of what happened, including the date of the breach and the date of discovery; a description of the types of unsecured PHR involved; steps individuals should take to protect themselves; a description of what the breached entity is doing to investigate, mitigate, and prevent future harm; and contact procedures for affected individuals to ask questions, including a toll-free telephone number, email address, website, or postal address.

[6] Like the FTC rule, the HHS rule only requires notification of media when 500 or more affected individuals are residents of the same jurisdiction or state.

[7] Identical to what the FTC rule requires for breaches involving less than 500 individuals, HHS requires that a log of breaches be maintained and provided to HHS each calendar year.

Continued on page 2...

New Health Security Breach Notification Rules . . .

Continued from page 1...

covered entity investigates and has a good faith belief that the person that accessed the information "was not able to retain such information."[8] The FTC rule provides no such exception to the definition of an incident requiring notification.

Implications

Many entities that use or maintain personal health information have longstanding security measures in place in order to comply with the HIPAA security rule. However, data that is secured in accordance with the HIPAA security rule still may be breached in a manner that would trigger the notification obligations required under the new rule. To the extent that the HIPAA security rule and the HIPAA breach notification rule have some overlap, organizations subject to each will need to undertake an individual analysis to ensure they comply with both.[9]

Entities may find themselves subject to both sets of regulations in much the same way that many businesses have found themselves subject to multiple privacy- and security-related requirements where they operate in more than one business sector or have more than one source of regulation. For example, a vendor that offers PHR to customers of a HIPAA-covered entity as a business associate and also offers PHR directly to the public, may be subject to both the HHS rule and the FTC breach notice rule. For some of these situations, compliance guidance issued by the FTC suggests that the goal is to ensure that affected consumers receive at least one notification in the event of a breach.

With respect to managing the data supply chain and the layers of potential notification obligations, the FTC encourages covered entities, business associates, and vendors to allocate breach notification responsibility in advance by contract. The agency further encourages notifications to come from the organization that has a direct relationship with the affected individuals. As a practical matter, in the wake of breach notification statutes in virtually all of the states,[10] many organizations already have begun to allocate these risks and responsibilities in the latest versions of their service agreements, privacy- and security-related exhibits, and in business-associate agreements. The new regulations add another layer of required legal analysis to situations experienced by so many businesses in the last few years.

The new rules suggest the ongoing importance of monitoring legal and regulatory developments in this area to help ensure that compliance and risk-management procedures are current and can be implemented in a timely manner while enabling a business to continue operating. The rules, coupled with continuing increased privacy regulations, reiterate the value of creating written incident-response policies to help coordinate responses. And finally, the agencies' guidance and commentary make clear the value to all businesses in planning for these issues not only as compliance matters, but also as part of their ongoing procurement processes.

ARRA's latest breach notification requirements reflect a continuing federal trend to regulate data privacy matters by sector with these most recent notification rules for health-related information following earlier regulation for financial data and the handling of customer proprietary network information by telecommunications carriers. Like these other industries, it seems likely that all members of the health data supply chain can expect increased emphasis on privacy and data protection in their contracts and should be prepared accordingly. As a practical matter, coupled with other recent changes to HIPAA, many organizations, especially business associates, may choose to review their existing policies and compliance programs as well as their risk management strategies for handling health-related data.

Wilson Sonsini Goodrich & Rosati attorneys regularly assist clients with all aspects of their privacy and information governance needs, including HIPAA compliance evaluations, security incident response, and incident avoidance. For additional information about the new rules and related questions, please contact Lydia Parnes at lparnes@wsgr.com or (202) 973-8801; Gerry Stegmaier at gstegmaier@wsgr.com or (202) 973-8809; or Wendy Devine at wdevine@wsgr.com or (858) 350-2321.

WSGR

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on September 24, 2009.
To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com

[8] 45 C.F.R. §164.402

[9] It is important to note that the new rule does not relieve HIPAA-covered entities and business associates from their previous HIPAA compliance obligations. Thus, they must comply both with this new rule and the HIPAA security rule.

[10] The ARRA provides that state breach notification laws are preempted by the FTC and HHS rules. However, preemption only applies to the extent that the requirements imposed by the state laws are *contrary* to those imposed by the new rules. The reality is that many state laws impose more detailed notification requirements than those mandated by the FTC and HHS rules; these requirements, such as specific language that must be contained in the notifications and provision of additional notice to the applicable state Attorneys General office, are arguably not contrary to, and thus not preempted by, the FTC and HHS rules.