

Security Breach Notification Rules Announced by HHS and FTC

In late August 2009, the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) issued regulations implementing provisions of the HITECH Act. The HITECH Act is part of the larger economic stimulus bill, the American Recovery and Reinvestment Act, which was passed in February 2009. The interim final rule written by HHS requires entities regulated by HIPAA such as hospitals, insurers and even certain financial institutions to notify affected persons when the security of their protected health information (PHI) has been breached. By contrast, the final rule published by the FTC requires vendors of personal health records (PHRs), such as Google Health and Microsoft Health Vault, and related entities to notify affected persons when the security of their individually identifiable information has been breached. The HHS and FTC rules are officially effective Sept. 23, 2009, but both HHS and the FTC have stated that they will not enforce the rules until February 22, 2010, the date that the rest of the HITECH privacy and security standards go into effect.

The HHS Rule

The rule published by HHS closely tracks the statutory language of HITECH with respect to security breaches, except that the rule creates a new “risk of harm” threshold, which will be discussed in further detail below.

Generally, under the rule, a HIPAA-covered entity must, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured PHI has been or is reasonably believed by the HIPAA-covered entity to have been accessed, acquired, used, or disclosed as a result of such breach. In the event of a breach, a HIPAA-covered entity must provide notice of such a breach “without unreasonable delay” and not later than sixty calendar days after discovery of a breach. The rule dictates that a breach is considered “discovered” by the HIPAA-covered entity as of the first day on which the breach was known to the HIPAA-covered entity, or, by exercising reasonable diligence, would have been known to the HIPAA-covered entity. The breach notification requirement applies regardless of the number of individuals whose PHI may have been affected by a breach of unsecured protected health information, but its applicability is limited to those breaches which trigger a “risk of harm” threshold, which will be discussed below.

If a HIPAA-covered entity should discover a breach of unsecured information, under the HHS rule, it must notify each individual whose unsecured PHI has been, or is reasonably believed by the HIPAA-covered entity to have been accessed, acquired, used or disclosed as a result of such breach “without unreasonable delay” and no later than sixty calendar days after discovery. The HHS rule requires that the notice contain specific information, including a brief description of the occurrence of the breach, a description of the types of information that were involved in the breach, steps that individuals should take to protect themselves from potential harm resulting from the breach, what the HIPAA-covered entity is doing to mitigate harm from the breach and contact procedures for affected individuals. In the event that over five hundred individuals of a particular state or jurisdiction are affected by a breach, the HIPAA-covered entity must notify the media of that state following discovery. Additionally, HHS must be notified no later than sixty calendar days following discovery in the case of breaches affecting more than five hundred individuals and annually in the case of breaches affecting less than five hundred individuals. No later than sixty calendar days after discovery of a breach of protected health information, a business associate of a HIPAA-covered entity must notify such HIPAA-covered entity, which, in turn, must notify affected individuals.

Under the HHS rule, “breach” is defined as the acquisition, access, use or disclosure of PHI that violates HIPAA’s Privacy Rule and compromises the security or privacy of protected health information. The HHS rule specifically excludes the following from the definition of breach: 1) any good faith, unintentional acquisition, access, or use of PHI by an employee or person acting under the authority of a HIPAA-covered entity or a business associate that does not result in further use or disclosure; 2) any inadvertent disclosure by a person who is authorized to access PHI at a HIPAA-covered entity or its business associate to another person authorized to access PHI at the HIPAA-covered entity or its business associate that does not result in further use or disclosure; and (3) a disclosure of PHI where a HIPAA-covered entity or its business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

After receiving numerous comments indicating that (i) HHS should align the rule with many state breach notification laws that require entities to reach harm thresholds before providing notification and (ii) failure to include a harm threshold for requiring breach notification may diminish the impact for notifications received by individuals (either because an individual may be flooded with notifications or would be caused to panic about relatively insignificant breaches), HHS drafted clarifications in the rule to address these concerns. The HHS rule contains a “risk of harm” threshold, which provides that an entity regulated by HIPAA consider the potential harm of a breach of unsecured information before triggering notification requirements in the rule. Thus the phrase “compromises the security or privacy of protected health information” within the definition of “breach” is defined as “poses a significant risk of financial, reputational, or other harm to the individual.” To determine whether such a risk of harm exists, HIPAA-covered entities and business associates are required to carry out risk assessments upon discovery of a breach. In performing such a risk assessment, HIPAA-covered entities and business associates should consider factors including who impermissibly used the information and to whom it was impermissibly disclosed as well as the type and amount of PHI involved in the impermissible use or disclosure.

In the final interim rule, HHS repeated guidance it published in April 2009 with respect to what constitutes unsecured and secured protected health information. Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS, such as encryption. While encryption is not required under HIPAA, by encrypting protected health information, a HIPAA-covered entity or business associate can ensure that PHI is secure. A HIPAA-covered entity or business associate that experiences a breach of encrypted PHI is not required to provide notification to any affected individuals because such information is not “unsecured.”

The FTC Rule

The FTC Final Rule is similar to the language of the HITECH Act. It applies to breaches of unsecured PHR-identifiable health information (“PHR identifiable health information” has the same definition as “individually identifiable information” under HIPAA) It differs from the HHS rule in that it does not apply to the entities governed by the HHS rule, i.e. HIPAA-covered entities or entities acting in the capacity of business associates. Rather, it applies to vendors of PHRs, PHR-related entities and third party service providers such as entities that provide billing, debt collection or data storage services and includes non-profit entities (traditionally outside the scope of the FTC’s jurisdiction). PHR vendors and PHR-related entities, however, could also be business associates in different contexts, so there is an overlap between the FTC and HHS rules in certain situations. As a result, the reach of the FTC rule combined with the HHS rule is potentially quite broad. The FTC rule, like the HHS rule, states that PHR identifiable health information that is encrypted is not “unsecure”, and therefore no breach notification is required if encrypted PHR identifiable health information is breached.

Also similar to the HHS rule, vendors of PHRs and PHR-related entities, under the FTC rule, are required to notify affected individuals upon discovery of a breach of unsecured PHR identifiable health information. A third party service provider that experiences such a breach must notify its contracted PHR vendor or PHR-related entity (it must also notify any HIPAA-covered entity with which it has a business associate agreement). PHR-related entities are those entities which are not already HIPAA-covered entities or are acting as business associates that: (1) offer products or services through the website of a vendor of personal health records; (2) offer products or services through the web site of HIPAA-covered entities that

offer PHRs; or (3) access information in a personal health record or send information to a personal health record. A third party service provider is an entity which provides services related to the maintenance of a PHR and “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.”

The FTC rule, like the HHS rule, mandates that a PHR vendor’s or a PHR-related entity’s notice to individuals affected by a breach of unsecured PHR identifiable health information contain a description of the events that led to the breach and the type of information involved (e.g. Social Security number, disability code, etc.), steps individuals can take to protect themselves from further harm, what the PHR vendor or PHR-related entity is doing to mitigate harm from the breach and contact procedures for affected individuals. Such notice must be sent “without unreasonable delay” and in no case later than sixty calendar days following discovery of such breach. The PHR vendor or PHR-related entity must also notify the FTC with a form found at the following website: <http://ftc.gov/os/2009/08/R911002hbnform.pdf>. If five hundred or more people are affected, then the PHR vendor or PHR-related entity must notify the FTC within ten days of discovering the breach. If fewer than five hundred people are affected, then the PHR-related entity must notify the FTC no later than sixty calendar days after the beginning of the following calendar year. If five hundred or more people are affected in a given state, then the PHR vendor or PHR-related entity must notify the media in that state.

The FTC rule creates a presumption that if unauthorized access of unsecured PHR identifiable health information occurs, it includes unauthorized acquisition of such unsecured PHR identifiable health information as well unless the vendor of PHRs, 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, unauthorized acquisition of such information. It does not, however, employ a risk of harm threshold, like the threshold present in the HHS rule. While an entity can rebut the presumption that unsecured PHR identifiable health information was not acquired, and therefore notice to affected individuals is not required, the default assumption under the FTC rule is that notification with respect to any breach of such information is required to be sent to affected individuals.

Next Steps for Healthcare Entities

A breach of unsecured health information can cause serious reputational damage to a business or provider of services in the healthcare sector. The best way to avoid triggering breach notification requirements is for healthcare entities to engage in preemptive compliance. Healthcare entities— from hospitals and insurers to e-health technology vendors as well as financial institutions that use and disclose PHI — should amend their policies and procedures to comply with the HHS and FTC rules. Employees of such businesses should be trained to identify what constitutes a breach of unsecured PHI and/or unsecured PHR-identifiable information and how best to avoid triggering breach notification requirements in the first place. HIPAA-covered entities, business associates, PHR vendors and PHR-related entities should consider encrypting personal health records if they are handling PHI in situations where there is potential for security breaches. Also, HIPAA-covered entities should amend their contracts with business associate to ensure that their business associate agreements reflect the new HHS breach notification requirements.

If you have questions regarding this Alert, please contact [Linda A. Malek](mailto:Linda.A.Malek@mosessinger.com) at 212.554.7814/ Lmalek@mosessinger.com, chair of Moses & Singer’s [Healthcare](#) practice, or [Jay D. Meisel](mailto:Jay.D.Meisel@mosessinger.com) at 212.554.7823/ jmeisel@mosessinger.com.

MOSES & SINGER LLP

Attorneys in the [Healthcare](#) practice have extensive experience working with managed care organizations, not-for-profit healthcare systems, hospitals, academic medical centers, integrated delivery systems and physician practices that range from individual physicians to large, multi-specialty group

practices and clinics. We also represent IPAs, ancillary providers (including laboratories, pharmaceutical, radiology and others), physician and dental practice management companies, e-health companies, government entities, long-term and home health care entities, hospices and other forms of alternative delivery systems.

Since 1919, [Moses & Singer LLP](#) has provided legal services to diverse businesses and to prominent individuals and their families. Among the firm's broad array of U.S. and international clients are leaders in banking and finance, entertainment, media, real estate, healthcare, advertising, and the hotel and hospitality industries. We provide cost-effective and result-focused legal services in the following primary areas:

- Advertising
- Banking and Finance
- Business Reorganization, Bankruptcy and Creditors' Rights
- Corporate, Securities and M & A
- Employment and Labor
- Entertainment
- Healthcare
- Hotel and Hospitality
- Income Tax
- Intellectual Property
- International Trade
- Internet/Technology
- Legal Ethics & Law Firm Practice
- Litigation
- Matrimonial and Family Law
- Privacy
- Private Funds
- Promotions
- Real Estate
- Trusts and Estates and Wealth Preservation

The Chrysler Building
405 Lexington Avenue
New York, NY 10174-1299
Tel: 212.554.7800 Fax: 212.554.7700

2200 Fletcher Avenue
Fort Lee, NJ 07024
Tel: 201.363.1210 Fax: 201.363.9210
Abraham Y. Skoff, Esq.
Managing Attorney for New Jersey

Disclaimer

Viewing this document or contacting Moses & Singer LLP does not create an attorney-client relationship.

This document is intended as a general comment on certain developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This document contains information that may be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

Attorney Advertising

It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.

Copyright © 2009 Moses & Singer LLP
All Rights Reserved