

Executive Summary

The first Federal privacy breach notification regulations were mandated by provisions in the American Recovery & Reinvestment Act of 2009 (ARRA). This Act required the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) to draft regulations for notification in case of a breach of Protected Health Information (PHI). Both HHS and the FTC have taken steps to issue regulations on breach notification. The Privacy and Security Committee of the Minnesota e-Health Initiative, coordinated by the MN Department of Health, has taken a lead in providing public comment and trying to make sure the two rules are aligned.

HHS has issued a guidance on breach notification. The HHS guidance applies to Covered Entities and Business Associates¹. This guidance was published for public comment on April 17, 2009 and HHS will be publishing the interim final regulation by August 17, 2009. Follow this link for the full text of the guidance, <http://www.health.state.mn.us/e-health/hitech/ht042009hhssecurity.pdf>.

The FTC has issued a proposed regulation - "16 CFR, Part 318 -Health Breach Notification Rule." The FTC rule applies to vendors of Personal Health Records (PHR), "PHR related entities," and third-party service providers to these entities that have access to unsecured PHR. Examples of "PHR related entities" are web applications that help individuals manage their health and or a vendor that provides health supplements or services to individuals with health issues. The proposed FTC rule can be accessed at <http://www.health.state.mn.us/e-health/hitech/ht041609phrbreach.pdf>.

Definitions in the two rules are substantially the same. And the FTC and HHS are attempting to make sure the two rules are in agreement. The public comment period is over for both rules.

Highlights of HHS Guidance on Breach Notification

- Individuals must be notified of any breach of their unsecured PHI. A breach is defined as "unauthorized access, use, or disclosure." And unsecured PHI is defined as identifiable personal health information that has not been rendered unreadable by cryptology or destruction (shredding or burning).
- Notification must take place within 60 days of when the breach was discovered
- Notification must include a brief description of what happened, what types of PHI were involved, what the covered entity is doing about it, steps the individual can take to protect themselves, and contact information
- Notices must be sent to individuals via first class mail. Breaches of 500 or more records must be published in the local media. HHS must be notified immediately of breaches of 500 or more and provided an annual report of all breaches.
- "De-identified data," or records that cannot be linked to a specific person are not considered PHI
- Secured PHI must use encryption that meets current NIST standards

¹ **Covered Entities** include: Hospitals, clinics, physicians (including medical and chiropractic doctors, optometrists, dentists, radiologists, podiatrists, and nurse practitioners), pharmacies, health insurers, self-insured companies, and certain government agencies and non-profits

Business Associate: These are vendors and business partners of covered entities that process EPHI.

Highlights of FTC Proposed Rule on Health Breach Notification

- The FTC requires vendors of personal health records and PHR related entities, upon discovery of a breach of security, to provide notification to individuals whose information was breached
- Notification must take place “without unreasonable delay” and before 60 days expires, unless a delay is requested by law enforcement officials.
- Failure to discover a breach that could have been discovered with “reasonable” security precautions is a violation of the rule
- The rule does NOT apply to entities that are covered by HIPAA or to the entities’ activities as a business associate to a HIPAA covered entity. For example, “a website offering an online personalized health checklist; and a brick-and-mortar company advertising dietary supplements online” would be covered under the FTC rule. But a company providing the same services to the members of a health plan would be a “Business Associate” and covered under the HHS rule.
- The FTC definition of breach uses the term ‘acquired’ whereas the HHS uses “accessed, used, or disclosed.” These differences have been pointed out and will hopefully be clarified in the final versions.
- One new wrinkle is that in some cases just the customer list of a vendor, that only contains names and other normally public information, may be considered PHI. “ For example, the theft of an unsecured customer list of a vendor of personal health records or related entity directed to AIDS patients or people with mental illness would require a breach notification, even if no specific health information is contained in that list.” (FTC 16 CFR Part 318)

Recommendations

1. Stay tuned. Public comment has ended on both the HHS Guidance and the proposed FTC rule. Both agencies will be issuing breach notification regulations by August 17, 2009.
2. Any organization that is a HIPAA Covered Entity, provides business services to a HIPAA covered entity that involve access of PHI, or processes personal health records in any form should carefully study the two breach notification rules. If there is any doubt whether the rules relate to an organization we strongly suggest obtaining a legal opinion.
3. If your organization does not currently have a breach notification plan and either of these regulations may apply, we strongly recommend that you develop a plan and the capability to implement it.

An Aeritae R&D Report

*Aeritae R&D conducts technical and market research in the fields of Information Risk Management (IRM), Service Management, IT Architecture and IT Infrastructure and taps a network of industry advisors in the Twin Cities region to gain technical and market intelligence. Aeritae R&D will periodically publish “**Aeritae Advisory**” reports on subjects of interest to the regional IT industry.*