

Health Information Breach Notification Rule

The Federal Trade Commission (“FTC”), as required under the American Recovery and Reinvestment Act of 2009, has published a notice of proposed rules and request for comments regarding requirements for vendors of personal health records (“PHR”) and related entities to notify individuals when the security of their individually identifiable health information is breached. These rules apply to vendors of personal health records, personal health record entities and third party service providers which are not subject to the privacy and security requirements of HIPAA. Part of the FTC’s request for comments concerns what vendors or other entities would be subject to this rule. Definitions of PHR related entities, third party service providers and vendors of PHR are given in the rule. If such vendors engage in activities as business associates of HIPAA covered-entities such entities will be subject only to HIPAA requirements.

This proposed rule defines breach of security as “the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, 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.”

This proposed rule requires vendors of personal health records and PHR related entities, upon discovery of a breach of security, to notify U.S. citizens and residents whose information was acquired in the breach and to notify the FTC. It also requires third party service providers to both vendors of personal health records and PHR related entities to provide notification to such vendors and entities (including a senior official) following the discovery of a breach. A breach is treated as discovered as of the first day on which such breach is known to a vendor of personal

health records, PHR related entity, or third party service provider.

This rule also proposes that notification of the breach to both individuals and the media to be made “without unreasonable delay” and in no case later than 60 calendar days after discovery of the breach. The FTC shall receive notification from vendors of personal health records and PHR related entities as soon as possible and in no case later than five business days following the date of discovery of the breach if the breach involves the unsecured PHR identifiable health information of 500 or more individuals. If the breach involved fewer than 500 individuals, the vendor of personal health records or PHR related entity may maintain a log of any such breach occurring over the ensuing twelve months and submit the log to the FTC.

In addition, this proposed rule provides the information needed for notification purposes as well as the methods of notification of a breach to individuals, the FTC and the media in the event of a breach of unsecured PHR identifiable health information.

For more information please contact Popovits & Robinson at 708/479-3230.

This publication is for the general information of clients and friends of Popovits & Robinson. It does not provide legal advice for any specific matter. Popovits & Robinson excludes all liability with respect to any part of this document, including without limitation, any errors or omissions.