Federal Trade Commission Issues Final Breach Notification Rule

On August 17, the FTC voted to approve a final breach notification rule, which will require web-based vendors of personal health records (PHRs) and entities offering third-party applications for PHRs to notify consumers when a breach of electronic health information (EHR) has occurred. The American Recovery and Reinvestment Act (ARRA) requires the Department of Health and Human Services (HHS), in consultation with the FTC, to conduct a study and submit a report by February 2010 detailing potential privacy, security, and breach notification requirements for vendors of health information that are not covered by the Health Insurance Portability and Accountability Act (HIPAA). Until this study is completed, ARRA required the FTC to issue a breach notification rule for these entities. The FTC published a proposed rule in April 2009.

The final rule requires vendors to notify consumers directly in the case of a breach. Service providers to these entities will be required to notify the vendor of a breach who, in turn, will be required to notify the consumer. If a breach involves 500 or more people, a vendor must notify the media as well as the consumers. The FTC must also be notified in the case of a breach.

ARRA allows entities normally outside of the FTC's jurisdiction to be subject to the breach notification rule. In addition, the final rule authorizes the FTC to recover civil monetary penalties from entities that fail to comply with the rule.

The final rule will be published in the Federal Register in the near future. Currently, the final rule can be accessed through the FTC's website. The FTC has also created a form for use after breaches. It specifies the timing, method, and content of the notification.

Final Rule: http://www.ftc.gov/os/2009/08/R911002hbn.pdf

Health Breach Notification Form: http://www.ftc.gov/os/2009/08/R911002hbnform.pdf