

## HIPAA Enforcement Provides Template for Enforcement of Upcoming "Red Flag Rules" Requirements for Identity Theft Prevention Programs

Data breaches at healthcare enterprises are increasingly frequent, and healthcare providers need to create and pursue programs aimed at minimizing the risks of data breaches, and respond well to a breach. The Federal Trade Commission (FTC) and other federal regulatory agencies have issued the so-called "Red Flag Rules," which outline the basic contours of a comprehensive identity theft prevention program that affected entities must implement. The type of identity theft which the Red Flag Rules seek to discourage in the context of the health care industry is the misuse of another individual's previously stolen identity to obtain health care services or goods, or to obtain money by using the stolen identity to falsify claims for medical services. The FTC has delayed enforcement until May 1, 2009 of the Red Flag Rules requirement to develop and implement a sufficient identity theft prevention program. This date is fast approaching.

In addition to the encroaching requirements of the Red Flag Rules, health care providers still must comply with other, more traditional requirements regarding the maintenance of protected health information (PHI). These requirements include the Privacy and Security Rules imposed under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The HIPAA Privacy and Security Rules oblige covered entities to safeguard the privacy of PHI and to honor security standards regarding patient information maintained in electronic form. The U.S. Department of Health and Human Services has settled claims against a group of non-profit health care corporations regarding alleged violations of the Privacy and Security Rules through the execution of a corrective action plan (CAP), in which the entities agreed to implement a broad data breach prevention program. This CAP provides some insight into how the federal government may respond to healthcare organizations alleged to have violated the upcoming Red Flag Rules requirements.

These issues, and some of the steps which a health care organization should take to secure protected data under both HIPAA and the Red Flag Rules, are explained in an article by Peter Hardy and Vadim Schick, "Preventing Data Breaches: HIPAA Compliance and the Red Flag Rules," published in the April 2009 edition of Compliance Today, and accessible via this [link](#).

Peter and Vadim will also discuss related issues of significant new expansions in data privacy protection laws, including under HIPAA and the Red Flag Rules, in a free webinar on April 7, 2009 at 10 a.m. To register for this webinar, entitled "Preparing for the Breach: Significant Expansions in Data Privacy Laws," please click the following link: [Register Now](#).

Post & Schell's Data Protection Group provides the range of legal skill sets you will need for front-end compliance or breach remediation. We have nationally recognized health data security lawyers, experienced former prosecutors to address questions of fraud and law enforcement, and sophisticated compliance lawyers who know how to put "action" into your corrective action plans.

If you have any questions or comments about this E-Flash, please contact Peter D. Hardy at 215-587-1001 or at [phardy@postschell.com](mailto:p Hardy@postschell.com), or Vadim Schick at (202) 661-6945 or at [vschick@postschell.com](mailto:vschick@postschell.com).

**Disclaimer:** this E-flash does not offer specific legal advice, nor does it create an attorney-client relationship. You should not reach any legal conclusions based on the information contained in this E-flash without first seeking the advice of counsel.