LAW OFFICES OF
GOODELL · STRATTON
EDMONDS & PALMER
ESTABLISHED 1881 LLP

By: Nathan D. Leadstrom, Partner
And
Mary E. Christopher, Associate Attorney

Medical Identity Theft: Is Your Office Ready to Comply with the Red Flag Rules?

Identity theft is devastating and generates financial consequences to both consumers and businesses. Surprisingly, Kansas ranks 29th in the number of identity thefts per capita.[1] Medical identity theft is one of the fastest growing forms of identity fraud. Although the Department of Health and Human Services is promoting the use of electronic health information technology to improve patient outcomes and minimize errors, digitization of consumer information may result in more opportunities for exploitation.[2]

The two most common means of perpetrating medical identity fraud include the use of another's identity and insurance information to swindle medical services, and capturing or purchasing personal health identification information to orchestrate large-scale health insurance billing frauds. While the HIPAA privacy regulations provide some protection for personal consumer information, HIPAA fails to provide adequate means of mitigation to victims of medical identity theft.[3]

In the wake of massive data breaches and the misuse of consumer information, the Federal Trade Commission and bank regulatory agencies issued federal identity theft regulations known as the "Red Flag Rules" and the "Address Discrepancy Rule."[4] The Red Flag rules require businesses to design and implement programs to detect, prevent, and mitigate instances of consumer identity theft. Both rules require mandatory compliance by November 1, 2008. [*Note: after this article was submitted for publication, the FTC granted a six-month delay of enforcement until May 1, 2009.*]

Many physicians and medical clinics may not yet realize they may be required to comply with these new rules. Because these regulations were issued by federal agencies that oversee financial institutions, health care providers may believe the rules are only for banks, lending agencies, and other creditors. That is not necessarily the case.

---

[1] According to the Federal Trade Commission's Consumer Fraud and Identity Theft Complaint Data for 2007.

[2] Michael Bologna, "Health Information Medical Identity Theft Becoming Widespread National Fraud Problem," 17 BNA's Health Law Reporter 1089 (August 14, 2008).

[3] Id.

[4] See 72 Fed. Reg. 63718 (Nov. 9, 2007). The Address Discrepancy rule requires any user of a nationwide credit report to develop and implement reasonable policies and procedures to enable the user to deal with an address discrepancy notice from a credit bureau. The user must implement reasonable policies and procedures for furnishing the reporting agency with verification of the consumer address if verification can reasonably be confirmed. *See* Robert Gellman and Pam Dixon, "Red Flag and Address Discrepancy Requirements," World Privacy Forum, September 24, 2008, p. 20.

The Red Flag Rules apply broadly to any "creditors" with "covered accounts," including some health care providers. As explained in a recent Federal Trade Commission Business Alert, "creditors" include "any entity that regularly extends, renews, or continues credit" or "that regularly arranges for the extension, renewal, or continuation of credit."[5] A "covered account" includes an "account [used] primarily for personal, family, or household purposes, that involves or is designated to permit multiple payments or transactions," or "[a]ny other account . . . for which there is a reasonably foreseeable risk . . . [of] identity theft." In other words, if a medical provider maintains credit accounts permitting patients to make multiple payments over time, that provider may be deemed to be a "creditor" offering a "covered account" that may be subject to the Red Flag rules.[6]

A well-designed Red Flag program should include procedures for:

(1) identifying risk factors and sources of identity theft;
(2) detection of Red Flags in connection with the opening of covered accounts and existing accounts;
(3) appropriate responses to a Red Flag commensurate with the degree of risk presented;
(4) periodic updates to reflect changing risks from identity theft and new safety measures; and,
(5) administrative oversight by the board of directors, a committee of the board, or designated senior employee.[7]

Medical providers are already required under HIPAA to have in place appropriate safeguards to protect the privacy of protected health information.[8] These are a good starting point to review to determine if they are sufficient to meet the requirements of the Red Flag Rules. With the guidance of an experienced health care attorney, it may be possible to design dovetail a Red Flag program so that it dovetails with the administration of existing HIPAA safeguards.

Even if a provider is not strictly required to comply, developing policies that guard against patient identity theft are a good business protection practice. The old adage an ounce of prevent is worth a pound of cure is ever present in this situation as the total costs of a breach, including the harm to your business's reputation, will likely greatly outweigh the costs of such a program.

This article was originally published in Vol. 1 No. 4 of Greater Kansas MD News published by Sunshine Media, Inc.

---

[5] "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft," FTC Business Alert, *available at* http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm/

[6] *See* Robert Gellman and Pam Dixon, "Red Flag and Address Discrepancy Requirements," World Privacy Forum, September 24, 2008, p. 7.

[7] *See* Federal Trade Commission, et al. Identity Theft Red Flags and Address Discrepancies Under the fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. (November 9, 2007) p. 63773, *available at* http://www.ftc.gov/os/fedreg/2007/November/071109redflags.pdf.

[8] 45 C.F.R. sec. 164.530(c).