BALCH & BINGHAM LLP

Alabama • Georgia • Mississippi • Washington, D.C.

HEALTHCARE BULLETIN

October 16, 2008

NEW IDENTITY THEFT 'RED FLAG' RULES APPLY TO HEALTHCARE PROVIDERS

Several federal agencies, including the Federal Trade Commission ("FTC"), recently issued joint rules and guidelines ("Red Flag Rules") aimed at detecting, preventing and mitigating identity theft as part of the Fair and Accurate Credit Transactions Act of 2003. These Red Flag Rules create certain requirements that most healthcare providers need to comply with by November 1, 2008.

Identity theft can cause serious financial consequences to consumers in the healthcare industry, FTC Division of Privacy and Identity Protection's Naomi Lefkowitz noted during a recent American Health Lawyers Association Teleconference. Ms. Lefkowitz added that identity theft not only causes financial harm to patients, but it can also put patients at risk, especially where patient information is co-mingled in medical records.

The Red Flag Rules require that each "creditor" that offers or maintains a "covered account" develop and implement a written Identity Theft Prevention Program. Any person or entity that defers payment for goods or services, such as by billing in arrears for medical treatment, will be considered a creditor, according to the FTC. Consequently, most healthcare providers will fall within the Red Flag Rules broad definition of a creditor simply by billing patients after rendering services.

Further, most healthcare providers offer or maintain covered accounts, defined as consumer accounts: (i) involving multiple payments or transactions; or (ii) for which there is a reasonably foreseeable risk of identity theft, including financial, operational, compliance, reputation, or litigation risk. The agreement of a healthcare provider to provide services on a recurring basis and accept payment afterwards creates a covered account. Also, each patient medical record held by a healthcare provider might be considered a covered account because it contains information at high risk for identity theft.

Thus, because most healthcare providers qualify as creditors that offer or maintain covered accounts, many providers will need to develop and implement an Identity Theft Prevention Program to comply with the Red Flag Rules.

Requirements for Identity Theft Prevention Programs

Identity Theft Prevention Programs must be in place by November 1, 2008, which is the date that the Red Flag Rules become effective.

Prior to drafting a program, healthcare providers may wish to consider assembling a team to perform an identity theft risk assessment. The team should include individuals from different departments of the provider and review (i) how an individual's identity is verified when opening an account during admission, (ii) what information is gathered, (iii) how that information is stored, and (iv) what steps could be taken to detect and prevent identity theft in connection with existing accounts.

To comply with the Red Flag Rules, a healthcare provider must develop a written program that identifies and detects the relevant warning signs – or "red flags" – of identity theft. The FTC has grouped potential red flags into five (5) categories, including:

- alerts, notifications, or warnings from a consumer reporting agency;
- suspicious documents;
- suspicious personally identifying information, such as a suspicious address;
- unusual use of, or suspicious activity relating to, a covered account; and
- notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the creditor.

Healthcare providers can ask various state agencies for help in identifying red flags as well. For example, the Board of Pharmacy or state healthcare associations will have had experience with patient complaints or fraud schemes.

Identity Theft Prevention Programs must also describe appropriate responses that would prevent and mitigate identity theft. Mitigating identity theft may mean that the healthcare provider has a system in place to notify patients or law enforcement of suspicious activity in patients' accounts. Further, healthcare providers should educate employees and patients regarding their Identity Theft Prevention Programs. Employees should be able to identify warning signs of identity theft. Patients should trust that their healthcare providers make the effort to verify patient identity and safeguard information.

Identity Theft Prevention Programs must be approved by the board of directors of the healthcare provider. Programs then should be managed by either the board of directors or a senior employee of the healthcare provider. Programs should include appropriate staff training, provide oversight of service providers, and be updated annually to ensure their effectiveness and attempt to catch new identity theft schemes.

Healthcare providers should ensure that contractors, such as third party agents, participate in their Identity Theft Prevention Programs through contract language specifying that the contractor complies with Red Flag Rules or that the contractor agrees to comply with the hospital's program.

Healthcare Providers Need Not Panic

Most healthcare providers likely have measures in place upon which to base their Identity Theft Prevention Programs. Many of the measures that healthcare providers took to comply with the HIPAA Security Rule may carry over into their Identity Theft Prevention Programs. For instance, a healthcare provider's security officer may head up its Identity Theft Prevention Program. The Red Flag Rules are designed to be flexible so that each Identity Theft Prevention Program is appropriate to the size and complexity of the company to which it is tailored.

Finally, if the American Medical Association ("AMA") and several trade associations representing healthcare providers get their way, concerns about establishing an Identity Theft Prevention Program may become a moot point. AMA and the other trade associations are in the process of lobbying the FTC to stop viewing physicians as "creditors" for the purposes of the Red Flag Rules.

More detailed compliance guidance from the FTC on the Red Flag Rules will be forthcoming. For questions about compliance with the Red Flag Rules, you can contact RedFlags@ftc.gov.

***

Should you have any questions, please do not hesitate to contact one of our healthcare attorneys at the offices below.

H E A L T H C A R E C O N T A C T S

BIRMINGHAM, AL

Matthew A. Aiken
205.226.3425
maiken@balch.com

Colin H. Luke
205.226.8729
cluke@balch.com

Jack B. Levy
205.226.8750
jlevy@balch.com

MONTGOMERY, AL

Dorman Walker
334.269.3138
dwalker@balch.com

ATLANTA, GA

Richard D. Sanders
404.261.6020
rsanders@balch.com

Philip M. Sprinkle, II
404.261.6020
psprinkle@balch.com

GULFPORT, MS

H. Rodger Wilder
228.214.0412
rwilder@balch.com

JACKSON, MS

David M. Thomas, II
601.965.8157
dthomas@balch.com