



BALCH & BINGHAM LLP

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

HEALTHCARE BULLETIN

April 1, 2009

RED FLAG RULES COMPLIANCE DEADLINE SET FOR MAY 1, 2009

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 May 1, 2009.

Red Flags Apply to Healthcare Providers

Although the American Medical Association (“AMA”) lobbied against the application of Red Flag Rules to healthcare providers, the FTC stated that the plain language and purpose of the rules dictate that health care professionals are covered by the rules. The FTC reasoned 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.

Thus, most healthcare providers who act as “creditors” and offer or maintain “covered accounts”, as well as 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

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.



Identity Theft Prevention Programs must also describe appropriate responses that would prevent and mitigate identity theft. Further, healthcare providers should educate employees and patients regarding their Identity Theft Prevention Programs.

Identity Theft Prevention Programs must be approved by the board of directors of the healthcare provider and managed by either the board of directors or a senior employee of the healthcare provider.

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: Balch & Bingham Can Help

In an effort to assist healthcare providers to meet the Red Flag Rules requirements, Balch & Bingham LLP has created a Model Red Flag Program which includes template policies and procedures that meet Red Flag Rule requirements.

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

Dinetia Newman
601.965.8169
dnewman@balch.com

The Healthcare Bulletin is published as an informational resource for clients and friends of Balch & Bingham LLP. It does not contain legal advice, and is not a solicitation to perform legal services. No representation is made that the quality of legal services performed by Balch & Bingham LLP is greater than the quality of legal services performed by other lawyers. Design, logo, and content © 2009 Balch & Bingham LLP.

