

RED FLAG RULES AND THEIR APPLICATION TO PHYSICIAN PRACTICES

PREPARED BY JAMES A. CHRISTOPHERSON, ESQ.



**JAMES A. CHRISTOPHERSON, ESQ.
100 Park Street
Traverse City, MI 49684
(231) 929-0500
(231) 929-0504 - Fax
Email: christopherson@ddc-law.com**

BIOGRAPHICAL STATEMENT

James A. Christopherson of Dingeman, Dancer & Christopherson, PLC, represents physicians, physician practices, healthcare organizations, joint ventures, physician organizations, and ambulatory surgery centers. His practice includes advising clients regarding compliance issues, employment issues, litigation, corporate issues including formation, merger and succession issues, and tax exempt legal issues. He practices in the area of healthcare law, commercial litigation, and alternative dispute resolution. He received his B.A., *magna cum laude*, from Michigan State University, and his J.D. degree, *cum laude*, from Wayne State University School of Law, where he received an American Jurisprudence Award and the Silver Key Certificate. He is a member of the State Bar of Michigan and is admitted to practice before the United States Supreme Court (where he has personally argued), the United States District Courts for the Eastern and Western Districts of Michigan, and the United States Court of Appeals for the Sixth Circuit. He is a member of the American Health Lawyers Association, the Health Care Law Sections of the State Bar of Michigan, and the American Bar Association and several committees and working groups. He is a frequent author and speaker on healthcare issues. He has authored several law review articles including "Physician / Hospital Joint Ventures in the Wake of St. Davids" (Journal of Health Law, Winter 2004, Volume 37, No.1), "Buyer Beware When Purchasing a Medical Practice" (Michigan Health Law Report, Summer 2002) and "The Captive Medical Malpractice Insurance Company Alternative" (Annals of Health Law, Volume 5, 1998). He can be reached at christopherson@ddc-law.com or (231) 929-0500.

RED FLAG RULES

Under the authority of the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”), the Federal Trade Commission (FTC) and other federal agencies issued a set of rules published in the Federal Register on November 9, 2007 (72 Fed. Reg. 63718) that originally required financial institutions and creditors holding consumer or other “covered accounts” to develop and implement identity theft prevention program that complies with the regulations by November 1, 2008. These rules, commonly referred to as the “Red Flag Rules,” likely affect hospitals, individual physicians, physician groups, and other health care organizations that qualify as “creditors” based on its billing and collection practices.

The Federal Trade Commission (FTC) announced October 22, 2008 that it was delaying enforcement of key elements of its Red Flag Rules to allow “creditors” and financial institutions additional time to fully implement policies and procedures designed to thwart identity theft. In its Enforcement Policy Statement, the FTC noted that “Given the confusion and uncertainty within major industries under the FTC’s jurisdiction about the applicability of the rule, and the fact that there is no longer sufficient time for members of those industries to develop their programs and meet the November 1 compliance date, the Commission believes that immediate enforcement of the rule on November 1 would be neither equitable for the covered entities nor beneficial to the public.”

Duties regarding the detection, prevention, and mitigation of identity theft, codified as 16 C.F.R. §681.2, now will become enforceable on **May 1, 2009**, a six-month reprieve from the original enforcement deadline of November 1, 2008.

On their face, the Red Flag Rules seem aimed at financial institutions and other creditors that utilize sensitive personal information about a customer, accessed through a credit application process, and the protection of identity theft through the inappropriate use of an individual’s credit report. Due to the broad definition of a “creditor” however, the Red Flag Rules may apply to physician practices.

Under FACTA, the term “creditor” is defined as any entity that regularly extends, renews or continues credit; regularly arranges for the extension, renewal or continuation of credit or any assignee of an original creditor. Bottom line – **“Any person providing service or product for which the consumer pays after delivery is a creditor.”** Some staff attorneys in the Privacy and Identity Protection Section of the FTC have taken the position that physicians are “creditors,” and therefore subject to the Red Flag or final rules, if they do not require full payment up front at the time they see patients, but rather bill patients after the physician’s services are rendered. These staff attorneys are advising that physicians who accept insurance are considered “creditors” if the patient is ultimately responsible for the medical fees (as is routinely the case with respect to co-pays or deductibles or services not covered by insurance). Many physician organizations including the MGMA, AMA and others strongly disagree with the FTC’s interpretation that physicians are “creditors,” and have unsuccessfully attempted to have the FTC change its position.

Red Flags are those events that the FTC says should alert an organization that there is risk of identity theft. Red Flags can be determined by looking at the entity's own history of Identity Theft and the FTC's suggested list of red flags

Under the regulations, creditors holding covered accounts (qualified patient accounts), must develop an identity theft prevention program that includes reasonable policies and procedures for detecting, preventing and mitigating identity theft. The program should enable the healthcare organization to:

- Identify relevant patterns, practices and specific activities (Red Flags) that signal possible identity theft and incorporate those red flags into a written identity theft program that covers both new and existing patients;
- Detect actual Red Flags once the program has been implemented;
- Respond appropriately to detected Red Flags to prevent and mitigate identity theft; and
- Ensure the program is updated periodically to reflect changes in risks.

The Red Flag Rules require creditors to obtain approval of a compliant written identity theft program from its governing board or an appropriate committee of the board of directors by the **May 1, 2009** deadline. The Red Flag Rules identify twenty-six (26) Red Flags that are useful to incorporate into any identity theft prevention program, such as: (1) address discrepancy; (2) name discrepancy on identification or insurance information; (3) presentation of suspicious documents; (4) personal information inconsistent with information already on file; and (5) unusual use or suspicious activity related to a covered account.

Presently, the FTC has not announced active plans to audit organizations for compliance with the Red Flag Rules. However, an identity theft-related event such as a data breach, or an employee reporting non-compliance to the FTC or other governmental regulators, could open your practice up to monetary penalties and civil litigation. There are three areas of concern when discussing penalties:

- **Federal Trade Commission.** The FTC is authorized to bring enforcement actions in federal court for violations, and could enact penalties of up to \$2,500 for each independent violation of the Red Flag Rules.
- **State Enforcement.** States are authorized to bring actions on behalf of their residents and may recover up to \$1,000 for each violation, in addition to the recovery of attorney's fees.
- **Civil Liability.** Each consumer (patient) may be entitled to recover actual damages sustained from a violation.

The most immediate concern to address for providers that qualify as creditors is obtaining the appropriate internal organizational approval from your board of directors or an appropriate committee of the board for an initial identity theft prevention program that complies with the Red Flag Rules **prior to May 1, 2009**.

- Providers must be in compliance by **May 1, 2009**:
- A written plan must be approved by the board or an appropriate subcommittee.
- Provide training to employees and service providers that may access covered accounts.
- The board or an appropriate subcommittee must monitor the development, implementation, and administration of the program, receive annual reports on effectiveness, and approve any material changes.

If you have any questions about the Red Flag Rules or if you need help in preparing an Identity Theft Prevention Program, please contact Mr. Christopherson at christopherson@ddc-law.com or 231-929-0500.

The opinions expressed in these materials are intended for general guidance only. They are not intended as recommendations for specific situations. The laws, rules, regulations and statutes are subject to change. As always, please consult a qualified attorney for specific legal guidance.

S:\JAC\CD\INTERNET\2009 Webpage Articles\Red Flag Rules.doc