

## Red Flag Rule Compliance in Healthcare

### Overview

The Red Flag Rules are a result of the Fair and Accurate Credit Transaction Act and focus on the prevention of identity theft. Originally intended for financial institutions and creditors, the Red Flag Rules become applicable to healthcare entities because they are considered creditors. This document provides a high level overview of the Red Flag Rules and a timeline to prepare for the compliance deadline of May 2009.

### Requirements of the Regulation

A Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft. The Red Flag Rules state that healthcare entities must establish reasonable policies and procedures for implementing the identity theft guidelines.

In order to accomplish this, a healthcare entity must develop a written program to detect, prevent, and mitigate identity theft in connection with the opening of an account or any existing account. The written program must address four main points<sup>1</sup>:

- Identify relevant Red Flags for the covered accounts and incorporate those Red Flags into the Program;
- Detect Red Flags that have been incorporated into the program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

The Red Flag Rules are similar to the HIPAA regulations in that they are technology neutral. Each entity must decide what guidelines are appropriate for their operations and then develop policies and procedures accordingly. Red Flag requirements can be included in existing policies and procedures where practical. Healthcare entities should consider leveraging their HIPAA Risk Management process to include Red Flag requirements.

The administrative requirements for Red Flag Programs must include:

- Approval of the written Program by the Board of Directors or a committee of the Board;
- Oversight, implementation, and administration of the plan;
- Staff training; and
- Service Providers

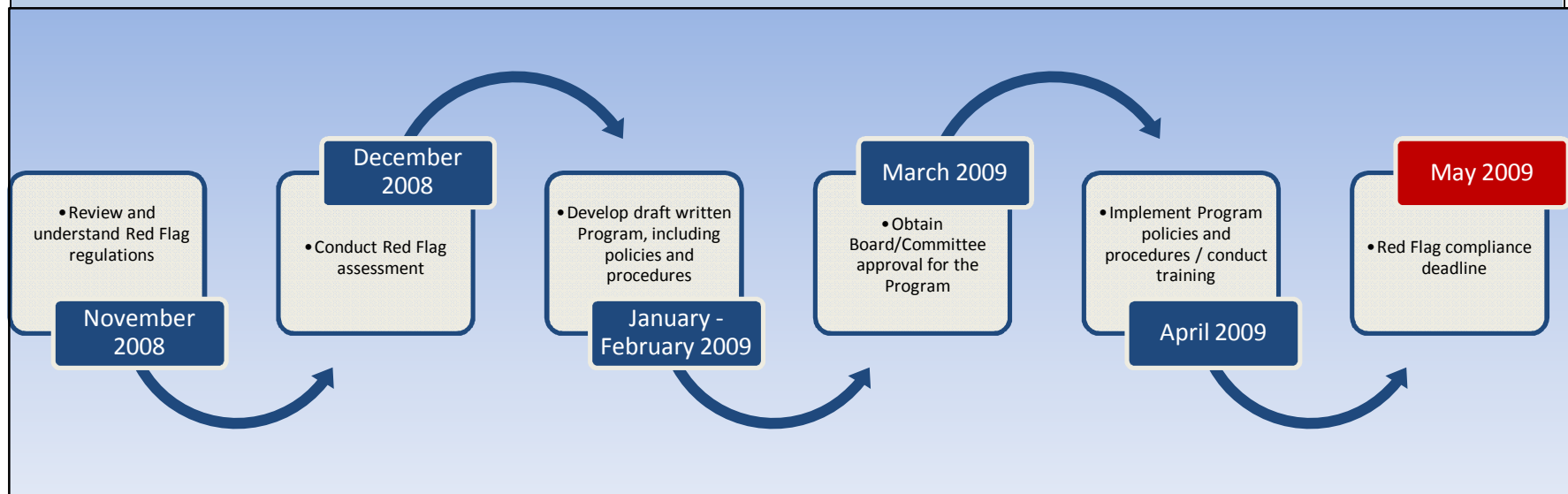
<sup>1</sup> Federal Register Vol. 72, No. 217, Page 63719-63720

## What to Do

Healthcare entities should begin by reviewing the Red Flag Regulations to understand how they apply to your organization. Conduct an assessment to use as baseline for the development of the written program. This assessment should include determining which covered accounts are offered, any previous experience with identity theft, which guidelines are appropriate, which Red Flags are relevant, and which accounts are most likely to have identity theft occur.

Once the assessment has been completed, a written Program must be developed that includes policies and procedures to address the appropriate guidelines and meet the compliance requirement. The Program should be submitted to the Board of Directors or committee of the Board for approval. Once the Program is approved, the healthcare entity should train employees on any changes to existing policies and procedures and any new policies and procedures that came from the program development. The entity should also implement any changes required by the Program. Moving forward, the Program should be reviewed and updated periodically. The Red Flag Program could be combined with the HIPAA compliance review process and completed in tandem.

## Timeline for Compliance



*This exhibit is representative of the tasks and timeline related to compliance with the Red Flag Rules. Healthcare Organizations have until the extended deadline of May 2009 to become compliant with the Red Flag Rules. If you have questions about the Red Flag Rules, contact Clint Davies ([cdavies@bdmp.com](mailto:cdavies@bdmp.com)) or Dan Vogt ([dvogt@bdmp.com](mailto:dvogt@bdmp.com)).*