

## RED FLAGS RULE UPDATE

On April 30, the Federal Trade Commission (FTC) announced that it will delay enforcement of the identity theft Red Flags Rule from May 1, 2009 to **August 1, 2009** giving more time for covered entities to develop identity theft prevention programs. The federal rules adopted pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) require covered providers to have programs to detect and respond to “Red Flags” – patterns, practices, or any specific activity that indicates a threat of identity theft. Penalties for willful noncompliance include the consumer’s actual damages (up to \$1000), punitive damages, and attorney fees.

Health care providers that regularly extend credit for services must comply with these regulations. For example, providers that allow patients to defer payment for services, or pay in installments, are subject to the new rules. Providers who are HIPAA covered entities will likely find that compliance with the Red Flags rule dovetails nicely with their existing privacy and security programs. Indeed, many of the same procedures providers use to protect health information may also be applied to protect against identity theft. However, even providers who are not HIPAA covered entities may be subject to the Red Flags Rule.

To comply with the Red Flags rule, your program needs five key components: Identify, Detect, Respond, Update, and Oversight. As with HIPAA compliance, the Red Flags rule gives providers flexibility in developing a compliance program suited to the size and complexity of their operations.

Providers should review their existing policies and procedures to identify possible risks to the security of account information, such as past history of data theft, suspicious activity, and outdated intake procedures. Providers should then implement a detection process to monitor change of address requests, patient authentication, and other instances where identity theft is possible. Providers are required to appropriately respond to instances of identity theft, such as cooperating with law enforcement, monitoring patient accounts, and changing passwords. The program should be reviewed at least annually and updated as needed to account for new technology, processes, and any incidents.

Your office should immediately adopt written policies and procedures to comply with the new rules. The Red Flag compliance program should be formally approved by the directors, and a management-level employee should be appointed to oversee the implementation and continuous updates needed to prevent evolving risks to patients’ personal information.

Feel free to contact B. Kevin Burgess or Jaclyn K. Semple at Watkinson Laird Rubenstein Baldwin & Burgess, P.C., at (541) 484-2277 in Eugene, (541) 673-5528 in Roseburg, (541) 923-8767 in Redmond, or (541) 757-1365 in Corvallis for further information.

Watkinson Laird Rubenstein Baldwin & Burgess, P.C.

