SMITH ANDERSON

Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

E-ALERT

Health Care Providers and Red Flags Rule Compliance: Implementing an Identity Theft Prevention Program by May 1, 2009

Who Must Comply with the Red Flags Rule?	The compliance date for the requirements of the Red Flags Rule pertaining to identity theft (the "Rule") is May 1, 2009, and health care providers that meet the qualifying criteria under the Rule will need to implement an Identity Theft Prevention Program (a "Program") by May 1, 2009. The Rule, which is published by the Federal Trade Commission ("FTC"), requires "*creditors*" that maintain "*covered accounts*" to implement a Program. The FTC recently responded to the American Medical Association's request for the FTC to support its reasoning for why health care providers are not excluded from complying with the Rule (a copy of the letter can be accessed at http://www.smithlaw.com/misc/1187453_1.pdf). The FTC confirmed its position that the plain language and purpose of the Rule dictate that health care providers would be covered by the Rule, and thus required to implement a Program if they regularly allow patients to defer payment for their services. If a provider regularly allows patients to defer payment until after professional services are provided, then the FTC would interpret the provider to be a creditor under the Rule. Billing a patient's insurer does not change the fact that the provider is allowing the patient to defer payment for services (assuming that the patient is ultimately financially responsible for amounts the insurer does not cover). However, accepting a credit card as payment for the services does not automatically make the provider a creditor. The Rule covers creditors that maintain covered accounts, which can include either: (i) an account that is offered or maintained primarily for personal, family, or household purposes and involves multiple payments or transactions; or (ii) an account for which there is a foreseeable risk to the consumer of identity theft. The FTC believes that patient accounts maintained by health care providers are increasingly the subject of medical identity fraud, and thus may qualify as covered accounts under the Rule. Penalties for not complying with the Rule include civil monetary penalties. Note that the Rule includes two additional sections that cover users of consumer credit reports and issuers of credit cards, both of which were effective as of November 1, 2008, but neither of which are addressed in this alert.
Steps to Take Prior to May 1, 2009	The FTC has stated that the Rule is flexible and a provider's Program should be based on the risk of identity theft to the particular provider. The FTC has issued guidelines to help creditors create and maintain a Program that satisfies the Rule (accessible at http://www.smithlaw.com/misc/redFlagsAlert_20090120092310.pdf). In addition, existing HIPAA privacy and security compliance programs can be incorporated into a provider's Program. Providers should also be aware of state laws related to the protection of consumer personal information, such as the North Carolina Identity Theft Protection Act of 2005.

	Steps for compliance with the Rule include the following: • A provider should determine whether it meets the definitions of a "creditor" that maintains "covered accounts" under the Rule. • If so, the provider should identify its covered accounts and analyze how they are opened, accessed, and maintained. The provider should also assess the risk of identity theft to its covered accounts, and its existing theft prevention measures. • The provider should review the list of "red flags" identified in the FTC guidelines and determine which red flags the provider should monitor. • Based on the red flags selected for monitoring, the provider should develop reasonable approaches for detecting such red flags when it opens new patient accounts and has transactions involving patient accounts. • The provider should determine what the appropriate responses will be if red flags are detected. • The provider should create written policies reflecting the processes set forth above and such policies must be approved by the provider's governing body. • Employees should be trained regarding the policies and any service providers granted access to covered accounts should be required to comply with the policies. • A person or board should be responsible for overseeing the policies and the policies should be monitored and updated at least annually. Health care providers are well advised to begin this process now as May 1, 2009 is fast approaching.	
For More Information, Please Contact:	Jennifer B. Markham Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P. 2500 Wachovia Capitol Center 150 Fayetteville Street Mall Raleigh, North Carolina 27602-2611 Telephone: (919) 821-6606 Fax: (919) 821-6800 Email: jmarkham@smithlaw.com	Alicia A. Gilleskie Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P. 2500 Wachovia Capitol Center 150 Fayetteville Street Mall Raleigh, North Carolina 27602-2611 Telephone: (919) 821-6741 Fax: (919) 821-6800 Email: agilleskie@smithlaw.com