



First Professionals Insurance Company



Anesthesiologists Professional Assurance Company

FREQUENTLY ASKED LEGAL QUESTIONS

What is the implementation compliance date for the Red Flags Rule (Rule)?

December 31, 2010

What is the purpose of the Rule?

To protect against identity theft. Identity theft occurs when someone uses another's personal identifying information (e.g., name, Social Security number, credit card number, or insurance enrollment or coverage data) to commit fraud or other crimes. In the case of physician practices, of particular concern is medical identity theft.

Who has to comply with the Rule?

The Rule applies to any institution considered a "creditor." A creditor is defined as "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit." The FTC, however, considers physicians who accept insurance or allow payment plans to be creditors and therefore subject to the Rule. The FTC takes the position that physicians extend credit by allowing deferred payment until services are rendered and insurance is collected.

How does the Rule differ from HIPAA privacy and security rules?

HIPAA is intended to protect personal health information (PHI) for security and privacy purposes. PHI as defined by HIPAA is covered by the Rule, but the Rule extends to other sensitive information such as credit card information, credit card information, tax identification numbers: Social Security numbers, business identification numbers and employer identification numbers.

What is a "red flag?"

A red flag is a pattern, practice, or specific account activity that indicates the possibility of identity theft. This includes alerts, notifications or warnings from a consumer reporting agency, suspicious documents and/or personal identifying information, such as an inconsistent address or nonexistent Social Security number, unusual use of, or suspicious activity relating to, a patient account, and notices of possible identity theft from patients, victims of identity theft or law enforcement authorities.

How can a medical/dental practice comply with the Rule?

The Rule requires "reasonable policies and procedures in place" to identify, detect and respond to identity theft "red flags." The definition of "reasonable" will depend on a practice's specific circumstances or specific experience with medical identity theft as well as the degree of risk for identity theft in the practice. These policies and procedures should complement existing HIPAA privacy and security policies and procedures that outline the administrative, technical and physical safeguards employed to ensure the security of patients' PHI.

Do compliance measures of the Red Flags Rule require a written Policy & Procedure?

Yes. The FTC Red Flags Rule requires implementation of a written Identity theft Prevention Program to include policy and procedure for identity theft protection.