



RED FLAGS RULE – COMPLIANCE POLICY

The implementation of the Federal Trade Commission's (FTC) Red Flags Rule has been postponed to November 1, 2009. To confirm that your practice provider qualifies as a creditor MEDTRON recommends practices check the FTC publication at <http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm> for information directly from FTC.

As a creditor, your practice is **required** to spot Red Flags that can be a sign of identity theft, possibly leading to Medical Identity Theft and develop a written 'Red Flags Program' to prevent, detect, and minimize damage from identity theft. **Basically, your practice must have a program in place to identify that a patient who receives services by your practice is really who they say they are.**

MEDTRON suggests:

Front Desk practices should require patients to present photo identification at each visit and scan the identification into the MEDTRON system via a card scanner. View the scanned photo id at each visit to confirm identification, i.e., to confirm same patient receiving care. If your practice does not have a card scanner, contact our Technical Dept at (985) 234-0500 or toll free at (866) 334-0500 or email at tech@medtronsoftware.com via double click at MEDTRON **Sign On** screen to order.

Hospital based practices must rely on hospital admitting procedure/policy therefore, coordinate with your facility.

'Flag' patient's accounts where inadequate identification has been provided, i.e., a patient presents without photo identification, information is presented that perhaps doesn't match **exactly** to their insurance card; patient refuses to completely fill out a new patient registration form; or patient advises their insurance card or driver's license is lost or forgotten. To 'Flag' such accounts, use a specific Account Status Code.

Refer to **User Guide: Account Status Codes**.

Remember **red flags** can occur after a patient visit. Suspicious scenarios:

Patient may call to complain about statements or insurance claims (*sent on behalf of your practice*) where the patient alleges he/she has never seen the rendering physician(s) **or** did not receive the service billed on statement or repeated returned mail as "Undeliverable", i.e., *the patient receiving statement was not patient who received service*.

Identifying and *flagging* patient's accounts with an Account Status Code specifically setup for red flags alerts your entire staff of possible concern when viewing the patient's account. Reports run based on the specific Account Status Code make it easy to identify and follow up and report any suspicious activity.

Please know that many of the HIPAA Security Policies and Practices MEDTRON has had in place since the implementation of HIPAA Security Rule in 2005 already protect patient data.

As further protection, MEDTRON implemented a system requirement of password changes every 180 days and a password **cannot** be reused from the previous four. Remember password must be a minimum of six (6) digits, maximum of ten (10) digits; must begin with a letter and contain at least one (1) number.

Users have the ability to change their password at any time within the 180 day requirement, should your practice policy require a more frequent change.

One of the most common security violations is the sharing or disclosing of one's user sign-on and/or password. Immediately alert MEDTRON of any newly hired or terminated employees and of any breach in security regarding the MEDTRON system.

To assist your practice in defining a policy, the AMA has created a sample **Red Flag Policy Template** that can be downloaded from the AMA website (<http://www.ama-assn.org/ama1/pub/upload/mm/368/red-flags-rule-policy.pdf>) and can be used as a guide in creating a policy unique to your practice. Please note that it is not the responsibility of MEDTRON/MEDDATA to enforce a practice to create a Red Flag policy, nor is it our responsibility to ensure that the practice's Red Flag rules are followed in accordance to federal law. MEDTRON is simply providing information to be used at the practice's discretion.