

FAIRWARNING®



FTC Red Flags Rule & FairWarning®

*The U.S. Federal Trade Commission has
re-enforced its position that the Identity Theft Red Flags Rule
applies to healthcare providers and physicians -
FairWarning® offers practical steps toward compliance with
the June 1st, 2010 deadline*

November 18, 2009

FairWarning, Inc.
United States of America
Phone: 727 576 6700
Web: www.FairWarningAudit.com
Email: info@FairWarningAudit.com

This document is meant to be general guidance for organizations which may be impacted by HIPAA and does not constitute legal advice. Copyright [FairWarning®](http://www.FairWarning.com), all rights reserved. If you read the document and have a recommendation on how to improve, correct or bring greater objectivity to the assessment, we ask that you send an email your suggestion to info@FairWarningAudit.com.

Summary

This document details how FairWarning® privacy monitoring solutions map to the FTC Red Flags Rule for healthcare. The document also details how healthcare providers and physician offices are taking practical steps in meeting the June 1st, 2010 deadline for FTC Identity Theft Red Flags Rule compliance by using FairWarning® privacy monitoring solutions. FairWarning® [customers](#) have presented on webinars as to how they are using FairWarning® privacy monitoring solutions to address key portions of the FTC rule as well as other healthcare compliance challenges such as HIPAA, SB 541, and AB 211. [Customer webinar materials](#) are available to the public.

The FTC Red Flags Rule and Healthcare

According to the United States Federal Trade Commission (FTC), beginning June 1st, 2010, physicians and healthcare providers must [comply](#) with the [FTC Identity Theft Red Flags Rule](#). In a nation-wide survey, the FTC found that 4.5 % of the 8.3 million victims of identity theft had experienced some form of medical identity theft. This translates to 373,500 patient lives that were verified to have been impacted by medical identity theft. The FTC also cited findings that the incidence of medical identity theft may be increasing.

The week of February 16th, 2009, the FTC re-enforced their position that healthcare providers and physicians must comply with FTC Identity Theft Red Flags Rule. Several medical associations had challenged position taken by the FTC on the applicability of the Identity Theft Red Flags Rule to physicians and healthcare providers. The FTC has spelled out in specifics why healthcare is bound by the rules.

New HIPAA Law Under the American Recovery and Reinvestment Act (ARRA) of 2009

The FTC news for healthcare comes at a time when all organizations that access protected health information (PHI) are facing new HIPAA privacy regulation as well as a dramatic increase in HIPAA enforcement law enacted by the ARRA of 2009 (Stimulus Bill). A FairWarning® companion document, [FairWarning® to ARRA 2009 New HIPAA Law mapping document](#) provides a detailed mapping of how FairWarning® [privacy monitoring solutions](#) address key components of the new HIPAA law.

With mounting privacy regulation and increased enforcement, healthcare providers are seeking solutions that provide return on investment (ROI) across multiple regulatory obligations. FairWarning® privacy monitoring solutions provide relief by addressing core components of the ARRA 2009 HIPAA law as well as portions of FTC Red Flags Rule.

FairWarning® & FTC Red Flags Rule

The [FTC Red Flags Rule for healthcare](#) provides general requirements aimed at identifying, detecting, mitigating and preventing behaviors associated with identity theft in the healthcare environment.

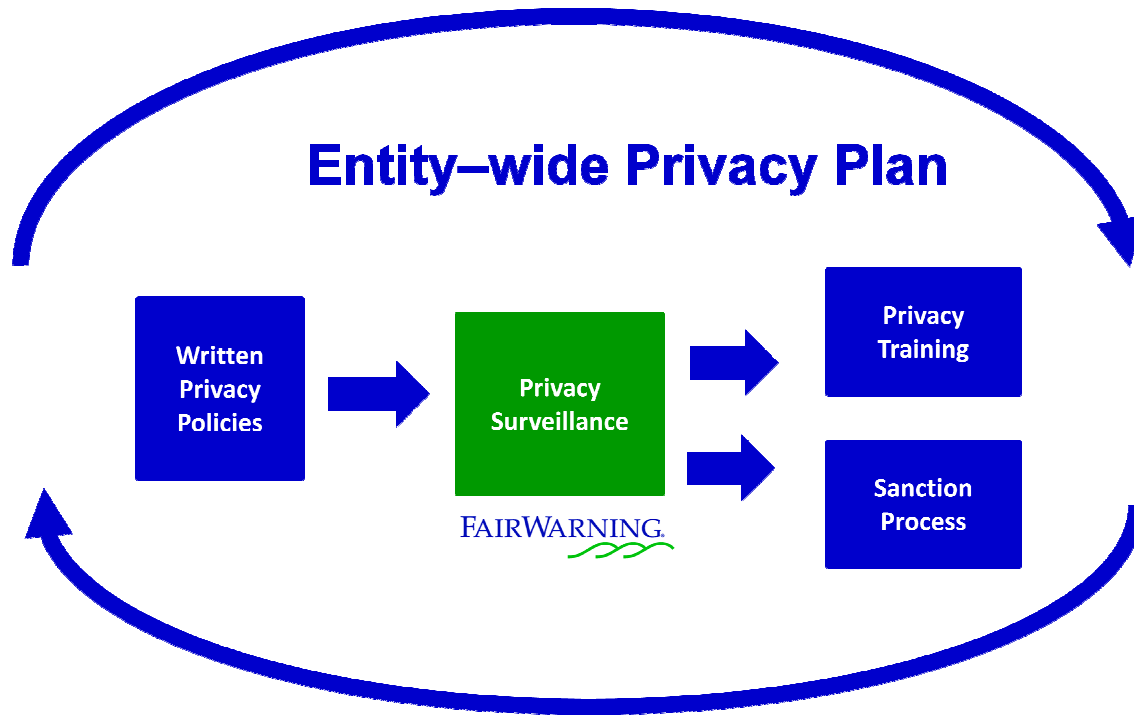
Identifying, detecting, mitigating and preventing identity theft in modern healthcare information technology environments is new to the industry and daunting challenge if taken on alone.

FairWarning® has worked with hundreds of healthcare providers to develop best practices for the detection and determent of identity theft in the healthcare environment. By leveraging [FairWarning® privacy monitoring solutions](#) to solve compliance and identify theft challenges such as those associated with HIPAA, AB 211, and SB 541, prudent healthcare providers can rapidly implement best compliance practices for the FTC Red Flags Rule. FairWarning® privacy monitoring solutions [automatically review the audit trails](#) of [Electronic Health Records](#) as well as other applications that access patient information.

How FairWarning® privacy monitoring solutions map to the FTC Red Flags Rule for healthcare is outlined in the table below:

FTC Red Flags Rule How to Comply	FAIRWARNING® OUT-OF-THE-BOX PRIVACY AUDITING
<p>Identify relevant red flags. Under the Rule, creditors and financial institutions with covered accounts must develop a written program to identify the warning signs of identity theft. This includes suspicious activity relating to a covered account.</p>	<ul style="list-style-type: none"> • FairWarning® provides dozens of automated best-practices for detecting identity theft within the healthcare EHR environment • FairWarning® provides proactive alerting & privacy dashboard, reporting, investigation • Automated, non-intrusive review of all audit sources that access Protected Health Information (PHI) • Dozens of audit sources supported out-of-the-box. Add entirely new audit source in eight (8) business hours
<p>Detect relevant red flags. Once you've identified the red flags that are relevant to your organization or business, you must establish policies and procedures to detect them in your day-to-day operations.</p>	<ul style="list-style-type: none"> • FairWarning® provides an automated, proactive patient & user incident detection • Ticket & reporting system to track potential incidents and their outcome
<p>Prevent and mitigate identity theft. Your program must include appropriate responses to your red flags to prevent and mitigate identity theft.</p>	<ul style="list-style-type: none"> • FairWarning® provides rapid patient and user investigation across all electronic health record systems and applications used to mitigate damages • FairWarning® provides point-and-click reporting capabilities to support rapid forensic investigation procedures
<p>Update your program periodically. Because identity theft threats change, your program must describe how you will update it to ensure that you are considering new risks and trends.</p>	<ul style="list-style-type: none"> • Use FairWarning® reporting and monitoring results to apply and re-enforce training processes. This re-enforcement allows organizations to keep their program updated.

Automatically, Detecting and Preventing Identity Theft in Healthcare



Re-enforced Culture of Privacy & Compliance

Other FTC Red Flags Rule Considerations

FairWarning® believes that while automating privacy monitoring is an essential element of detecting and preventing identity theft in healthcare, prudent healthcare providers will take a multi-pronged approach to implementing best practices for the sake of compliance, but more importantly to protect the safety of their patients.

There are additional considerations in complying with the FTC Red Flags Rule such as establishing consistent patient identification processes, regularly reviewing notices, billings, payments and credit records for patients. For more information, access the FTC web site at:

More on FTC Red Flags Rule for Healthcare

<http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm>

Deadline Information for Healthcare Providers and Physicians

<http://www.ftc.gov/opa/2008/10/redflags.shtm>

This document is meant to be general guidance for organizations which may be impacted by HIPAA and does not constitute legal advice. Copyright FairWarning®, all rights reserved. *If you read the document and have a recommendation on how to improve, correct or bring greater objectivity to the assessment, we ask that you send an email your suggestion to info@FairWarningAudit.com.*

About the Document

This document has been prepared by [FairWarning®](#), the world's leading supplier of healthcare [privacy monitoring solutions](#). FairWarning® [privacy monitoring solutions](#) are out-of-the-box, affordable, rapid to deploy and bring healthcare organizations into compliance with Federal and state laws such as HIPAA, AB 211, SB 541, FTC Red Flags Rule, PIPEDA, NHS Information Governance Toolkit, Caldicott Guardian Guidelines and others.