Reinhart

What the FTC's Identity Theft Rules (a.k.a. the Red Flag Rules) Mean for Health Care and Senior Housing Providers

When the Federal Trade Commission (FTC) published identity theft rules in November 2007 (also known as the "Red Flag Rules"), the event met with little fanfare from those in the health care community. As the FTC sought to clarify who was considered a "creditor" who must comply with the rules, however, it became clear that these rules would apply to many health care providers. The definition of a "creditor" extends far beyond just banks or credit card companies, and will encompass most entities that defer payment for the services they provide. Because of the breadth of this definition, health care and senior housing providers will need to evaluate whether they will be considered "creditors" and must comply with the rules.

Under the "Red Flag Rules," if a health care or senior housing provider is a "creditor" who maintains "covered accounts," the provider must develop an identity theft prevention program. Additionally, even if the provider is not a "creditor" it may be required to comply with the "Address Discrepancy Rule" if the provider uses consumer reports to make employment decisions or to assess a patient's ability to pay.

POSTED:

Jan 20, 2009

RELATED PRACTICES:

Health Care

https://www.reinhartlaw.com/practices/health-care

The Red Flag Rules

What Are Red Flags?

A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft. For example, Red Flags that providers might encounter could include patients or residents providing documents or information, such as insurance documents, addresses or social security numbers, that appear to be altered, forged or do not match information obtained from external sources such as credit reports.

The FTC's guidelines are designed to help entities identify relevant Red Flags and develop identity theft prevention programs, although not all of the Red Flags will apply to providers.[1]

Who Do the Red Flag Rules Apply To?

All materials copyright © 2025 Reinhart Boerner Van Deuren S.C. All rights reserved.

To determine whether they must comply with the Red Flag Rules, providers must assess whether they meet the definition of a "creditor" who maintains "covered accounts." A "creditor" is anyone who regularly extends credit (i.e., the right to defer payment for goods or services). This is a broad interpretation that encompasses a wide variety of situations in which a provider does not require payment at the time services are rendered. Even if the provider requires payment upon receipt of an invoice, it will still be considered a creditor if the invoice is not sent until after the services are performed.

A "covered account" is defined as (1) an account that the creditor offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft. This definition is also broadly interpreted and will apply to most relationships between health care providers and their patients or residents, as there is a continuing relationship between the health care provider and patient that permits the patient to obtain personal services, as well as a reasonably foreseeable risk to patients from identity theft.

What Do the Red Flag Rules Require?

Entities that are covered by the Red Flag Rules must develop and implement a written identity theft prevention program. Recognizing that the Red Flag Rules will apply to a wide variety of different entities, the rules require that the program must be appropriate to the size and complexity of the provider and the nature and scope of its activities. Therefore, the identity theft prevention program developed by a small community-based residential facility, whose staff know all of their residents by sight, will likely be less complex than a program developed by a hospital in a large city.

The identity theft prevention program must include reasonable policies and procedures to (1) identify relevant Red Flags, (2) detect Red Flags, (3) respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft, and (4) ensure the Program is updated periodically, to reflect changes in risks. The identity theft prevention program must involve the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the program. The provider must also obtain approval from its board of directors, or an appropriate committee of the board, for the written identity theft prevention program. The FTC regulations also require training staff,

All materials copyright © 2025 Reinhart Boerner Van Deuren S.C. All rights reserved.

as necessary, to effectively implement the program, and exercising appropriate and effective oversight of service provider arrangements.

After learning that many entities, including health care providers, were surprised that they would have to comply with the Red Flag Rules, the FTC decided to delay enforcing these requirements until May 1, 2009. Although it seems unlikely that the FTC will make health care or senior housing providers its top enforcement priority at first, providers who are covered by the rules should be prepared to demonstrate that they have taken reasonable efforts to comply with these regulations.

The Address Discrepancy Rules

In addition to the Red Flag Rules, the FTC also created new requirements for users of consumer reports. These rules are not as complex as the Red Flag Rules, and may apply to entities that use consumer reports even if they are not considered "creditors." It is important to note that the FTC has not delayed enforcement for these rules, which became effective on November 1, 2008.

Who Do the Address Discrepancy Rules Apply To?

These rules apply to any entity that uses consumer reports to make employment decisions or to assess a patient's or resident's ability to pay.

What Do the Address Discrepancy Rules Require?

Providers who are subject to these rules must develop reasonable policies and procedures to address situations when they request a consumer report and receive a notice of address discrepancy in response. If a provider requests a consumer report and receives a notice of address discrepancy, the provider must have policies and procedures designed to allow it to form a "reasonable belief" that a consumer report relates to the consumer about whom it has requested the report. Examples of such procedures include verifying the address with the consumer, reviewing the entity's own records, or verifying the address through third-party sources. The entity must also develop policies and procedures for providing an address to the consumer reporting agency for the consumer that the entity has reasonably confirmed is accurate, after it has received a notice of address discrepancy. These requirements are discussed at 16 C.F.R. § 681.1 and are very straightforward.

If you have any questions about the FTC's identity theft regulations, or would like

All materials copyright © 2025 Reinhart Boerner Van Deuren S.C. All rights reserved.

assistance in developing an identity theft prevention program, please contact one of Reinhart's health care attorneys in our Madison office by calling 608-229-2200 or in our Milwaukee office by calling 414-298-1000.

1See Appendix A of the published rule, available at

https://www.ftc.gov/policy/federal-register-notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and, located on pages 63773-74.

These materials provide general information which does not constitute legal or tax advice and should not be relied upon as such. Particular facts or future developments in the law may affect the topic(s) addressed within these materials. Always consult with a lawyer about your particular circumstances before acting on any information presented in these materials because it may not be applicable to you or your situation. Providing these materials to you does not create an attorney/client relationship. You should not provide confidential information to us until Reinhart agrees to represent you.

All materials copyright © 2025 Reinhart Boerner Van Deuren S.C. All rights reserved.