November 2017

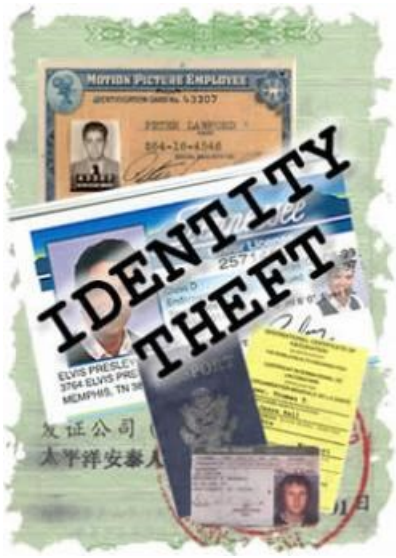
HEALTHTECH S3
strategy solutions support

COMPLIANCE NEWSLETTER

NAVIGATING THE MAZE

Cheri Benander, MSN, RN, CHC, NHCE-C
Health Services Consultant , HealthTechS3

MEDICAL IDENTITY THEFT



Has your facility implemented measures to prevent or reduce the risk of identity theft? An Identity Fraud Study conducted by Javelin Strategy & Research found that the identify fraud incidence rate has increased by sixteen percent.[1] Medical/healthcare organizations were affected by 377 breaches which was 34.5 percent of the total breaches.[2] These statistics reflect only those cases that were identified. According to the report, "These figures do not include the many attacks that go unreported. In addition, many attacks go undetected." [3]

Medical identity theft includes the use of your name or health insurance numbers to obtain medical care, prescription drugs, or even file claims with insurance providers.[4] Not only can this affect your patients financially, but if the thief's medical information becomes combined with theirs, the patient may receive improper or even life threatening medical care. Patients may be denied insurance due to inaccurate medical records and as you would expect, their credit can be damaged and their financial accounts drained. As a healthcare facility, you may be left with unpaid bills.

RED FLAGS RULE

A "Red Flag" according to 16 CFR 681.12(b)(9) is a pattern, practice, or specific activity that indicates the possible existence of identity theft. In an attempt to protect individuals from identity theft, the Federal Trade Commission (FTC) created a rule under the Fair and Accurate Credit Transactions Act called the Red Flags Rule. The rule passed on January 1, 2008 and was delayed until December 31, 2010.[5] The rule "...requires many businesses and organizations to implement an

identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage."[6] The requirements in the Red Flags Rule are aimed at Financial Institutions and creditors. The FTC offers the following questionnaire to determine if an organization is covered under the Red Flags Rule.

To determine if your organization is a creditor under the Red Flags Rule ask yourself the following questions:

Does my business or organization regularly:

- defer payment for goods and services or bill customers?
- grant or arrange credit?
- participate in the decision to extend, renew, or set the terms of credit?

If you answer:

- No to all, the Rule does not apply
- Yes to one or more, ask:

Does my business or organization regularly and in the ordinary course of business:

- Get or use consumer reports in connection with a credit transaction?
- Give information to credit reporting companies in connection with a credit transaction?
- Advance funds to-or for-someone who must repay them, either with funds or pledged property (excluding incidental expenses in connection with the services you provide to them)?

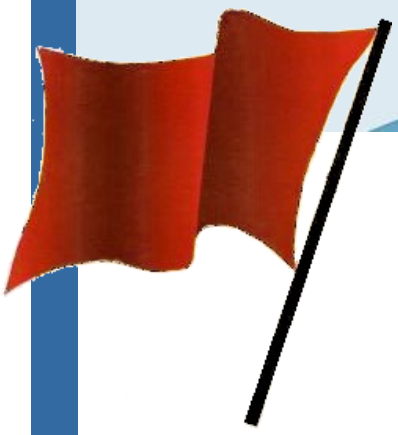
If you answer:

- No to all, the Rule does not apply
- Yes to one or more, you are a creditor covered by the Rule.[7]

Healthcare organizations that defer payments, set up payment plans or help patients get credit from other sources would be considered creditors under the rule. "On the other hand health care providers who require payment before or at the time of service are not creditors under the Red Flags Rule."[8]

If you meet the definition of a creditor, you then must determine if you have any covered accounts. These types of accounts are defined as "...a consumer account that allows multiple payments or transactions or any other account with a reasonably foreseeable risk of identity theft."[9]

Most healthcare providers will fall under the creditor definition, have covered accounts and be required to develop a program to deter identity theft. Whether or not you are "required" to develop a program or not, doing so will help to protect your patients and your business.



PROGRAM IMPLEMENTATION

16 CFR 681.1 (d)(2) describes the elements required in an Identity Theft Program and indicates that financial institutions or creditors who have covered accounts must develop policies and procedures that:

1. Identifies relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into is program;

2. Detects Red Flags that have been incorporated into the Program of the financial institution or creditor;

3. Respond appropriately to any Red Flags that have been detected to prevent and mitigate identity theft, and

4. Ensure the program is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

The rules further indicate that you will need to involve the board of directors, a committee of the board or a designated employee at the level of senior management in the oversight, development and implementation and administration of the program.[10] The written plan will need to be approved by either the board of directors or an appropriate committee of the board.[11] You will need to ensure

that there is appropriate oversight of services and provider arrangements that you train staff to effectively implement the program.[12]

CONCLUSION

Identify theft is on the rise. Thieves are constantly coming up with new ways to steal identities and obtain money and services fraudulently. Implementing a program will not only satisfy the requirements under the Red Flags Rule but it will also protect your patients, your business and federal funds.

[1] Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study. Available from: https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

[2] Facts + Statistics: Identity theft and cybercrime. Available from https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[3] Indem. para 7

[4] Medical identity theft. Available from https://www.consumer.ftc.gov/articles/0171-medical-identity-theft

[5] FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule. Available from https://www.ftc.gov/news-events/press-releases/2010/05/ftc-extends-enforcement-deadline-identity-theft-red-flags-rule

[6] Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business, para 6 Available from https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business#overview

[7] Indem.

[8] The "Red Flags" rule: What healthcare providers need to know, para 6. Available from http://www.modernmedicine.com/modern-medicine/news/modernmedicine/modern-medicine-feature-articles/red-flags-rule-what-healthcare-

[9] Indem para 7

[10] 16 CFR 681.1(e)

[11] 16 CFR 681.1(e)

[12] 16 CFR 681.1(e)

HealthTechS3 hopes that the information contained herein will be informative and helpful on industry topics. However, please note that this information is not intended to be definitive. HealthTech and its affiliates expressly disclaim any and all liability, whatsoever, for any such information and for any use made thereof. Recipients of this information should consult original source materials and qualified healthcare regulatory counsel for specific guidance in healthcare reimbursement and regulatory matters.

For more information, please contact Cheri Benander:
Cell: 307-202-0315
Main: 615-309-7421
cheri.benander@healthtechs3.com
5110 Maryland Way, Suite 200 | Brentwood, TN 37027
www.healthtechs3.com

HealthTechS3 is an award-winning healthcare consulting and hospital management firm based in Brentwood, Tennessee with clients across the United States. We are dedicated to the goal of improving performance, achieving compliance, reducing costs and ultimately improving patient care. Leveraging consultants with deep healthcare industry experience, HealthTechS3 provides actionable insights and guidance that supports informed decision making and drives efficiency in operational performance.