



## “Red Flags” Rule for Health Care Providers and Facilities

The Federal Trade Commission (FTC) began enforcing the Red Flags Rule on May 1, 2009. This will require many doctor’s offices, hospitals, and other health care providers and facilities to establish a written procedure to identify warning signs—or “red flags” - of identity theft. Medical identity theft occurs when a person using someone else’s identity and/or insurance information when seeking medical care. The FTC found that approximately 5% of identity theft victims have had some type of medical identity theft. The result often leaves victims with their medical benefits depleted and with inaccurate medical records which could result in possible life-threatening consequences. Health care providers are left with unpaid bills affecting their business as well.

Each health care provider and facility must assess their payment and billing procedures to see if they are affected by the Red Flags Rule. The law applies based on whether the provider’s payment and billing activities fall within the law’s definition of “creditor” and “covered account.”

If the provider is a “creditor” they may be subject to the Rule. The law defines “creditor” as to include any business that regularly defers payments for products or services or makes available the extension of credit. So, physician offices which bill patients after visits for the balance due and not reimbursed by insurance would be a creditor. Also, any health care provider which lets clients set up payment plans after the service, or assist in getting the patient credit from outside sources, is a creditor.

Providers and facilities which require payment in advance or at the time of service, or only accept payment from Medicaid or programs that the patient is not responsible for payment, are not creditors under the Red Flags Rule. In addition, taking credit card payments for service does not make the provider a creditor under the Rule.

“Covered account” is a consumer account allowing multiple payments/transactions that have a foreseeable risk of identity theft. Providers which have accounts for patients are generally “covered accounts” under the Rule. If the provider is a “creditor” with “covered accounts” they must create a written Identity Theft Prevention Program to identify and address the potential red flags which could result in identity theft.

There aren’t any criminal penalties for non-compliance with the Red Flags Rule, however, financial penalties can result. Compliance with the Rule reassures the patients of health care providers and facilities that the company is doing their part to protect their identity.

For more information go to: [www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf](http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf)

*Information from the Federal Trade Commission [www.ftc.gov/bcp/edu/pubs/articles/art11.shtm](http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm)*

## Cyber Liability for Health Care Clients

There are many different Cyber Liability products in the market. Many Cyber Liability policies provide coverage for Privacy, Identity Theft, Media, Electronic Theft, and Network Security Liability. Each health care provider or facility has different needs and those must be assessed when protecting against potential Cyber Liability incidents.

Some examples of health care Cyber Liability claim scenarios:

A health care facility has a network security breach. Patient records are stolen including financial and health benefits information. The stolen information is sold to individuals who in turn use the health benefits information to get medical services fraudulently. The patients whose identity were stolen sue the facility for emotional distress as well as for other damages. The insurance carriers sue the facility to recover the reimbursements made for the medical services obtained fraudulently.

A hospital provides patient records with online access. Information includes imagery, charts and laboratory information. Physicians subscribe for a fee to obtain access to the online patient records. A computer hacker obtains access to the network and corrupts the records on which physicians use to treat their patients. The doctors realize errors in the patient information and cannot treat the patients because of inaccurate records. The doctors sue the hospital for lost income because they were unable to treat patients.

There are many scenarios which apply to cyber liability, in this day and age, many work from home or send work emails to their personal email addresses to work on from home in the evenings or weekends. Data can be stolen or misdirected.

### COLORADO SPRINGS

800.397.9697  
719.528.8323

7011 Campus Drive #200  
Colorado Springs, CO  
80920

### CHICAGO

312.294.5532  
312.294.5493  
719.528.8323

550 W. Van Buren #1200  
Chicago, IL  
60607

### TAMPA

800.430.1050  
719.528.8323

3030 N. Rocky Point Dr. W.  
#161  
Tampa, FL  
33607

### Some coverages offered:

- Regulatory defense with no sub-limit
- Liabilities arising from the theft or loss of paper records
- Liability from identity theft and medical identity theft
- Media liability
- Electronic theft
- Recovery costs and extra expense
- Punitive damages (when insurable by law)
- Business interruption
- Threats or extortion
- Privacy notification

**Call us to discuss this option  
for your healthcare clients.**

**[www.hciusa.com](http://www.hciusa.com)**