

## **RED FLAG RULES AS A MEDICAL CLINIC.**

11/05/08

We will be following the so-called red flag rules.

These rules provide all financial institutions and creditors the opportunity to design an implemental program that is appropriate to their size and complexity.

We will pay attention, as a part of our implementation of this program to do the following:

1. Pay strict attention to alerts, notifications, or warnings from consumer reporting agency.
2. Check and recheck suspicious documents.
3. Check and recheck suspicious personally identifying information such as a suspicious address or a suspicious identification card.
4. If it all possible always obtain a picture labeled identification card with signature.
5. Pay attention to unusual use of, or suspicious activity related to, a cover account.
6. Pay attention to notices from customers, victims of identity theft, law enforcement authorities or other business about possible identity theft a connection with covered accounts.
7. We must identify relevant patterns, practices, and specific forms of activity that are considered “red flags” signaling possible identity theft and cooperate those red flags into the program.
8. We will detect as much as possible red flags that have been cooperated into our program of check and balances.
9. We will respond appropriate to any red flag that are detected to prevent and mitigate identity theft.
10. We will ensure that the program is updated periodically to reflect changes in risk from identity theft that we identify.
11. We will ensure that all personal data is appropriately placed in a HIPAA compliant dispose unit.

Kathy Roberts will coordinate all of the above security issues.

Kathy Roberts will identify and access any risk to customer information in each relevant area of this company’s operation and regularly evaluate the effectiveness of the current safeguards for controlling these risks. She will design and implement a safeguards program and regularly monitor and test it.

Kathy Roberts will and the company will select service provider that can maintain appropriate safeguards and she will make sure that our contract requires them to maintain safeguards and oversee their handing of customer information.

## **RED FLAG RULES AS A MEDICAL CLINIC**

11/05/08-2

Kathy Roberts and the company shall continually evaluate and adjust the program in light of any relevant changed circumstances, including changes in the firm's business or operations or the results of security testing and monitoring.

Kathy Roberts will regularly assess and address any risks to the patient/customer information and all areas of the companies operations including:

1. Employment management and training.
2. Information systems.
3. Detection and management of system failures.

Kathy Roberts as an office manager, together with \_\_\_\_\_ as our IT officer, shall ensure that information we are storing on our information systems is secure. Appropriate privacy and viral implementation shall be done.

Kathy Roberts shall also do the following:

1. Check references or background checks before hiring employees.
2. Ask every new employee to sign an agreement to follow company's confidentiality and security standards for handling customer information.
3. Limit access to customer information to employees who have a business reason to see it.
4. Controlling access to sensitive information shall be Kathy Robert's responsibility by requiring employees to use "strong" passwords, though it must be changed on a regular basis.
5. Password/activated screensavers should be employed to lock employee's computers after a period of inactivity.
6. Any at all lab talks, PDAs, cell phones, or other mobiles devices must be locked up before closing the office each evening.

Employees must be trained to:

1. Lock rooms where file cabinets are kept.
2. Not showing or openly posting employee passwords in work areas.
3. Encrypting sensitive customer information when it is transmitted electronically.
4. Referring calls or other requests for customer information to designate individuals who have been trained in how our company safeguard's personal data.
5. Reports suspicious attempts to obtain customer information to a designated personnel.
6. Regularly remind all employee's of our company's policy and the legal requirement thereof to keep customer information secure and confidential.
7. Employee disciplinary measures for security policy violations.
8. Prevent terminated employee's from accessing customer information by immediately deactivating their passwords and usernames with other appropriate measures taken with the cooperation of our IT personnel.

## **RED FLAG RULES AS A MEDICAL CLINIC**

11/05/08-3

9. Ensure that storage areas are protected against destruction or damage.
10. Store records in a room that is locked when unattended.
11. When an employee transmits credit card information or other sensitive financial data, secure sockets layer or other secure connections must be made so that information is protected in transit in cooperation with the IT personnel.

Kathy Roberts/the office manger shall dispose of customer information in a secure way and when applicable consistent with the FTC's disposal rule. Add [www.ftc.gov/os/2004/11/041118disposalfrn.pdf](http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf). This includes the necessity to burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.

It also includes the need to destroy or erase data when disposing of computer disc, CDs, magnetic tapes, hard drives, laptops, PDA, cell phones, or other electronic media.

The office manager shall be responsible, along with IT, in detecting and managing system failures. Effective security management requires our company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent the attacks, quickly diagnosing a security incident and having a plan and place for responding efficiently.

We will continue monitoring the websites.

Kathy Roberts/office manager shall continue monitoring the websites of our software vendors and reading relevant industry publications for news about emergent threats and available defenses. While maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information including the use of anti virus and anti spyware software and maintaining up-to-date firewalls with regular insurance that ports not use for our business are closed and that we promptly pass a long information and instruction to employees relevant to any new security risks or possible breaches.

The office manager/Kathy Roberts shall use appropriate oversight or order procedures to detect improper disclosure or theft customer information.

Kathy Roberts, in consultation with IT, shall use an up-to-date intrusion detection system to alert the office of attacks.

The office manager and IT shall monitor both in and out bound transfers of information for indications of compromise such unexpectedly large amount of data being transmitted from our business system to an unknown user.

## **RED FLAG RULES AS A MEDICAL CLINIC**

11/05/08-4

***Kathy Roberts shall insert a dummy account into each of our customer list and monitor the account to detect any unauthorized contacts or charges and take immediate action to secure any information that has or may have been compromised.***

Kathy Roberts or the office manager shall notify customers that their personal information are subject to a breach that pose the significant risks or risk of identity theft or related harm while also notifying law enforcement of the breach may involve criminal activity or there is evidence of the breach is resulted in identity theft or related harm. Further, the office manager/Kathy Roberts shall notify the credit bureaus and other business that may be affected by the breach.

When the compromise could result in harm to pertinent business, the police department should be called immediately. If the local police are not familiar with investigating information compromise, please contact the local FBI or US Secrete Service.

If names and social security numbers have been stolen, you should contact major credit bureaus for additional information or advice including Equifax at 1800-685-1111.

Experian email business records, victim assistance at experian.com

Trans Union phone# 1800-372-8391.

If the information compromise resulted from the improper posting or personal of information on our website, immediately remove the information from our site.

The office manager or Kathy Roberts shall be aware that internet search engines store or “cache” information for a period of time. The manager can contact the search engines to ensure that they do not archive personal information that was posted in err.

The office manager/Kathy Roberts shall be responsible for early notification to individuals whose personal information has been compromised along with them to take steps to mitigate the misuse of their information; in deciding if notification is warranted, consider the nature of the compromise that type of information taken, the likelihood of misuse and the potential damage arising from misuse. At the time of notification, the office manager shall describe to the client clearly what the manager knows about the compromise. Information must include how the compromise happened, what information was taken and how the thieves to the office manager’s knowledge, have used the information. In addition, the office manager shall communicate to the client what actions have been taken to remedy the situation. The client should be told how to reach any specific contact person in our organization. At the same time, the office manager shall consult with law enforcement and exactly what information to include in the office manager’s notice that does not hamper any investigation.

## **RED FLAG RULES AS A MEDICAL CLINIC**

11/05/08-5

*A model letter for notification of stolen identity can be found at the federal trade commission consumer protection site and title as “facts for business” to follow complaint or get free information on consumer issues the office manger can also consult [ftc.gov](http://ftc.gov) or call toll free 1877-FTC-HELP. Note that because the FTC has a law enforcement role with respect to information privacy, any one may seek guidance anonymously.*

Carey B. Dachman, M.D., S.C.