HCCS
Health Care Consulting Services

FINANCIAL POLICY & PROCEDURE

Subject: **Identity theft prevention and detection**
Red Flags Rule Compliance

Date: **April 1, 2009** **Approved by: Joanne Byron, CEO**
Update History: **May 1, 2009**

Our Policy to our Clients & Students

It is the policy of HCCS to follow all federal and state laws and reporting requirements regarding prevention of identity theft. Specifically, this policy outlines how HCCS will (1) identify, (2) detect and (3) respond to “red flags.”

Policy Posting

This policy will be posted on the HCCS web site www.hccsincorp.com for public viewing and inspection.

Definition of “Red Flag”

A “red flag” as defined by this policy includes a pattern, practice, or specific account or record activity that indicates possible identity theft.

Policy Updates: This policy will be reviewed and updated periodically, but not less than annually.

Approval: It is the policy of HCCS that this Identify theft prevention and detection and Red Flags Rule compliance program is approved by HCCS President & CEO as of April 1, 2009.

Privacy Official: It is the policy of HCCS that the Business Manager is assigned the responsibility of implementing and maintaining the Red Flags Rule requirements and added to the Business Manager's job description.

Sensitive Information: It is the policy of HCCS that, pursuant to the existing HIPAA Security Rule, appropriate physical, administrative and technical safeguards will be in place to reasonably safeguard protected health information and sensitive information related to patient identity from any intentional or unintentional use or disclosure.

Business Associates: HCCS does not conduct business with other vendors or organizations requiring the release of client or student demographic or payment information.

Staff Training: It is the policy of HCCS that all members of our workforce have been trained on the policies and procedures governing compliance with the Red Flags Rule. It is also the policy of HCCS that new members of our workforce receive training on these matters within a reasonable time after they have joined the workforce. It is the policy of HCCS to provide training should any policy or procedure related to the Red Flags Rule materially change. This training will be provided within a reasonable time after the policy or procedure materially changes. Furthermore, it is the policy of HCCS that training will be documented, indicating participants, date and subject matter.

Related Procedures

I. Identify red flags.

In the course of offering services to clients, HCCS may encounter inconsistent or suspicious documents, information or activity that may signal identity theft. HCCS identifies the following as potential red flags, and this policy includes procedures describing how to detect and respond to these red flags below:

1. A complaint or question from a client about information added to a credit report by our organization.

2. A dispute of a bill by a client who claims to be the victim of any type of identity theft.

3. A notice or inquiry from a fraud investigator for a law enforcement agency.

II. Identity Theft Prevention.

HCCS accepts personal and business checks that are dated with an authorized signature. We also accept credit card transactions by fax, mail and phone. These transactions are maintained in a confidential manner in our office.

Document Destruction: if a document containing credit card or client/student demographic information needs to be destroyed, HCCS will follow the HIPAA document destruction policy currently in place.

HCCS staff will be alert for discrepancies in credit card documents and patient information that suggest risk of identity theft or fraud. HCCS will follow this process when handling client's sensitive information (may include credit card information, address, and client or student information):

1. All new employees who will have access to sensitive information will undergo a credit report check upon hire.

2. Sensitive client information is kept away from public view in locked cabinets or drawers.

3. Unnecessary information is shredded or destroyed according to our HIPAA policy.

4. No sensitive information is taken via unsecured internet (ie, Email or unsecured Website).

5. Client information (sensitive or not) will only be given to people specifically authorized by the client.

6. Staff should be alert for the possibility of identity theft in the following situations:

    - The client submits identifying information that appears to be altered or forged.
    - Information on one form of identification the client submitted is inconsistent with information on another form of identification or with information already in the client's records.
    - An address or telephone number is discovered to be incorrect, non-existent or fictitious.
    - The client fails to provide identifying information or documents.

III. Responding to Red Flags.

If an employee of HCCS detects fraudulent activity or if a client claims to be a victim of identity theft, HCCS will respond to and investigate the situation. If the fraudulent activity involves protected health information (PHI) covered under the HIPAA security standards, HCCS will also apply its existing HIPAA security policies and procedures to the response. If potentially fraudulent activity (a red flag) is detected by an employee of HCCS:

1. The employee should gather all documentation and report the incident to his or her immediate supervisor.

2. The supervisor will conduct an investigation and report the concern to the CEO.

3. If the activity is determined to be fraudulent, then HCCS should take immediate action. Actions may include:
    - Cancel the transaction;
    - Notify appropriate law enforcement;
    - Notify the affected client; and/or
    - Assess impact to the company.

If a client claims to be a victim of identity theft:

1. The client will be encourages to file a police report for identity theft if he/she has not done so already.

2. The client will be encouraged to complete the ID Theft Affidavit developed by the FTC (Federal Trade Commission), along with supporting documentation.

3. HCCS will compare the client's documentation with personal information in the company's records.

4. If following investigation it appears that the client has been a victim of identity theft, HCCS will promptly consider what further remedial acts/notifications may be needed under the circumstances.

5. The CEO will review the affected client's record to confirm whether documentation was made in the client's record that resulted in inaccurate information in the record. If inaccuracies due to identity theft exist, a notation should be made in the record to indicate identity theft.

6. If following investigation it does not appear that the client has been a victim of identity theft, HCCS will take whatever action it deems appropriate.

Health Care Consulting Services, Inc
RISK ASSESSMENT

A) Determining if Your Facility is Subject to Red Flag Rules	**Creditor? Covered Accounts?**
A-1: Does your health care organization fit definition of "creditor"? Determining if your office is defined as a "creditor" applies to activities directly conducted by ***your office*** or through a ***third party medical billing service*** or ***collection agency*** where you send unpaid accounts used as an extension of your office. 1.1 Does your office help arrange for the extension, renewal, or continuation of credit?	🚩 Yes:☒ No: □
A-2: Does your health care organization offer "covered accounts"? 2.1 Explanation: payment plan options which permits patients or guarantors to pay balances through multiple payments or transactions over a given period of time.	🚩 Yes:☒ No: □
A-3: Use of Credit Reports? 3.1 Does your health care organization make use of or advocate the use of consumer credit reports for pre-employment purposes?	🚩 Yes:☒ No: □
3.2 Does your health care organization make use of credit reports to determine a patient's ability to pay, for skip tracing, qualifying for hardship, etc?	🚩 Yes:□ No: ☒
3.3 Does your health care organization use a billing or collection service as an extension of your office which uses credit reports?	🚩 Yes:□ No: ☒

Determination:

🚩 If "**NO**" was answered to ALL questions in Section A, you are NOT defined as a Creditor or have Covered Accounts. You do NOT need to proceed with this questionnaire. Keep this document and assessment as record that you have evaluated your organization. Re-evaluate quarterly to reassess if you are subject to the Red Flags Rule.

🚩 If "**YES**" to any item in Section "A", your organization is subject under the "**Red Flag Rule**" as a "creditor". ***Proceed to Sections B& C below***.

B) Red Flags / World Privacy Forum Suggested Pose Risk to Health Care Providers	**Risk Analysis Model** **Use company historical experience to determine Probability of Risk for each item.**
B-1 Records showing- - Service that is inconsistent with records as reported by the client.	Increasing Danger ➔ High Probability of Risk Low Danger High Probability of Risk High Danger ↑ Increasing Probability [✓ Low Probability of Risk Low Danger] Low Probability of Risk High Danger
B-2 A dispute of a bill by a client claiming - to be the victim of any type of identity theft.	Increasing Danger ➔ High Probability of Risk Low Danger High Probability of Risk High Danger ↑ Increasing Probability Low Probability of Risk Low Danger [✓ Low Probability of Risk High Danger]
B-3 Incidents where the wrong individual's credit card is charged: - causing a refund and recharge with the correct information	Increasing Danger ➔ High Probability of Risk Low Danger High Probability of Risk High Danger ↑ Increasing Probability Low Probability of Risk Low Danger [✓ Low Probability of Risk High Danger]
B-4 Incidents where client's personal information may be stolen: - credit card and/or personal information is left out for unauthorized access	Increasing Danger ➔ High Probability of Risk Low Danger High Probability of Risk High Danger ↑ Increasing Probability Low Probability of Risk Low Danger [✓ Low Probability of Risk High Danger]

C) Determining Implementation and Adequacy of written Identity Theft Prevention Program	**CHECKLIST** **Inventory of Action Required for Compliance**
C-1: Means to identify ***relevant*** red flags: Identifying relevant "red flags" for covered accounts and incorporating those red flags into an identity theft prevention policy. A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft. Please note that "consumer" may be referenced as "client" or "student". Examples of red flags include the following:	**Use this checklist as you progress with your written policy.**
1.1 Documents provided by the client that appear to have been altered or forged.	Yes: □ No: ☒
1.2 The use of a covered account in a manner that is not consistent with established patterns of activity on the account.	Yes: □ No: ☒
1.3 The return of mail sent to the client as undeliverable, although transactions continue to be conducted in connection with the account.	Yes: □ No: ☒
C) *Determining Implementation and Adequacy of written Identity Theft Prevention Program, Continued*	**CHECKLIST** **Inventory of Action Required for Compliance**
C-2: Does your Red Flag Compliance Policy meet **all four** requirements to the ***administration*** of the Identity Theft Prevention Program:	
2.1 Obtain approval of initial written program from its board of directors or a committee of the board;	Yes: ☒ No: □
2.2 Involve member(s) of the board of directors and/or employee at senior management in the oversight, implementation, development & administration of the program;	Yes: ☒ No: □
2.3 Train staff to effectively execute program;	Yes: ☒ No: □
2.4 Apply effective management of service provider arrangements.	Yes: ☒ No: □