TEXAS ASSOCIATION OF COMMUNITY HEALTH CENTERS, INC.
5900 SOUTHWEST PARKWAY, BUILDING 3
AUSTIN, TX 78735

Dawn McKinney
Director of State Affairs
National Association of Community Health Centers (NACHC)
Sent via email to dmckinney@nachc.com

April 9, 2009

Dear Ms. McKinney,

Attached along with this cover letter is a template policy and procedure addressing the requirements of the red flags rules for community health centers. All copyrights in the document are reserved by TACHC, but NACHC may distribute it to primary care associations around in the nation in its current format.

Please note in your distribution that the template policy and procedure is a slightly updated excerpt from the TACHC OC3 Manuals Updates published at the end of 2008. It therefore must be read with the knowledge that other parts of the TACHC OC3 Manuals and related trainings address how new policies and procedures must be reviewed and adopted and how health center staff should be notified about them and implement them. Access to the TACHC OC3 Manuals and related trainings can be found at http://www.tachc.org/About/Membership/Member_Directory/manuals.asp

Please also note that there are state, local or site specific requirements that health centers in other states may need to consider in adapting this template to their locations.

Feel free to call me if you have any questions.

Sincerely,

José E. Camacho

Att.: Template Policy and Procedure Regarding Identity Theft

PHONE:
(512) 329-5959

FAX:
(512) 329-9189

INTERNET:
WWW.TACHC.ORG

[Insert Name of Center]

Policy and Procedure

Regarding Identity Theft

I. Background

The Federal Trade Commission (FTC) has issued regulations known as the "Red Flags Rules" requiring creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. Where Centers defer payment for goods or services, they, too, are to be considered creditors. The identity theft program of a Center must provide for the identification, detection, and response to patterns, practices, or specific activities - known as "red flags" - that could indicate identity theft. FTC enforcement of these rules is set to begin May 1, 2009.

Under the Red Flags Rules, Centers must develop a written program that identifies and detects the relevant warning signs of identity theft.[1] The program must describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Executive Director, include appropriate staff training, and provide for oversight of any staff with access to patient identifying information.[2]

The FTC is concerned with medical identity theft, i.e. when someone uses another person's name and sometimes other parts of their identity, such as insurance information or Social Security Number, without the victim's knowledge or consent, to obtain medical services or goods. This could be harmful to an existing or future Center patient's health as well as their finances and the Center's.[3]

II. Policy

It is the policy of the Center to implement an Identity Theft Prevention Program. The Center will:

- Identify relevant Red Flags for those accounts for patients designed by the Center to permit multiple payments or

---

[1] The Red Flag Rules do not require the center to change what information is requested from patients at registration.
[2] The Center may meet some of these requirements with its HIPAA policies and procedures.
[3] For more information about Medical Identity Theft, see the World Privacy Forum's ***Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers*** posted at www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf

transactions;

- Detect those Red Flags as they arise;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically, to reflect changes in risks of identity theft to patients or to the safety and soundness of the center from identity theft.[4]

III. Procedure

The Center Board will approve this identity theft prevention policy and procedure, and the Executive Director will oversee its implementation. On a regular basis, a report will be made by the Executive Director and/or the Compliance Officer to the Board about the work of the Identity Theft Prevention Program.

Through its Privacy and Security policies and procedures, the Center has ensured as much as reasonably possible that a patient's protected health information (as defined under HIPAA) is only accessed by Center staff authorized to do so. The Center hereby identifies the following indicators of identity theft and requires staff authorized to access patient protected health information to report the detection of these indicators.

- The presentation of suspicious documents.
  - Records showing medical information that is inconsistent with the physical examination or a medical history as reported by the patient.
- The presentation of suspicious personal identifying information.
  - A Social Security number supplied by an applicant that is the same as that submitted by another patient.
  - Known patient returns to Center presenting a different name than before without explanation.
  - A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
- Notice from patients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with patient account.
  - Notification to Center by the patient or by repeatedly undeliverable mail that the patient is not receiving billing statements.
  - A complaint or question from a patient based on the patient's receipt of:

[4] See Federal Register, Vol. 72, No. 217, Friday, November 9, 2007 at p. 63720 *et seq.* for requirements.

- a bill for another individual;
- a bill for a product or service that the patient denies receiving;
- a bill from a health care provider that the patient never saw;
- a notice of insurance benefits for health services never received.

- Any other activity indicating identity theft of a Center patient or identity theft used to become a Center patient.

The Center will add to this list any other indicators that have led, in the Center's experience, to the discovery of identity theft at the Center.

The Center will communicate the requirement to all staff members and third parties that are authorized to access patient accounts to document any sign of identity theft, including those items on this list, and share it with the Finance Director and/or Executive Director immediately after detection. The Executive Director or his or her designee will investigate the sign of identity theft. If there is a credible factual basis for concern verified by the Executive Director, s/he or his or her designee will follow up with the patient to see if the transaction at issue was authorized by the patient. If that was not the case, the Executive Director work with the patient and Center staff to ensure the patient's health and billing information is that patient's only and is secured physically and electronically to the extent reasonably possible. The documents found to be affected by identity theft will be labeled as such, with incorrect information in them stricken (not erased or deleted) and amended if possible; if amendment is not possible, a new record will be created for the Center patient and the record affected by identity theft will be labeled as such and stored in a segregated file.

If there is a repeated problem with a patient's identity or account, and especially if there is evidence that the identity theft from or by a Center patient was successful, the Executive Director will discipline, up to and including termination where appropriate, any staff member and/or other patient involved in the perpetration of identity theft. When necessary, the Executive Director will also report the matter to the proper authorities locally and/or to the FTC.[5] Finally, the Center will not bill any third party for services the Center is aware were procured by identity theft.

[5] To report identity theft, call the FTC Consumer Response Line at 1-877-FTC-HELP. The FTC will contact the victim to assist them in addressing the identity theft and keep information in a database for other federal agencies and local law enforcement to access.