Unique Identifier: HWP 12075	DAY KIMBALL HOSPITAL Hospital-Wide Policy Manual Section – Leadership Page 1 of 9
TITLE: Privacy Protection – Red Flags Identity Theft Program	RESPONSIBLE PARTY (IES): Director, Quality/Risk Management Board of Directors President/CEO
FORMERLY KNOWN AS:	
EFFECTIVE: 3/31/09	REVISED:
REVIEWED:	
REGULATORY STANDARD:	

I. GENERAL STATEMENT OF PURPOSE:

To protect the confidentiality of personal information of employees, patients, and other clients of Day Kimball Hospital and its affiliates. This policy is established to comply with Federal Trade Commission "Red Flag Rule" regarding identify theft, and Connecticut Public Act No. 06-167 "An Act Concerning the Confidentiality of Social Security Numbers". The purposes of the program are to:

1. Identify the relevant Red Flags based on the risk factors associated with the Hospital's covered accounts;

2. Institute policies and procedures for detecting Red flags;

3. Identify steps the institution will take to prevent and mitigate Identity Theft; and

4. Create a system for regular updates and administrative oversight to the program.

II. POLICY STATEMENT:

It is the policy of Day Kimball Hospital to protect the confidentiality of personal information obtained and used in the course of business from its employees, patients, and other clients.

Day Kimball Hospital will maintain reasonable policies and procedures to detect and mitigate identity theft related to personal information received or maintained by Day Kimball Hospital for the purposes of obtaining reimbursement for services.

This program supplements, but does not replace or supersede, any policies, procedures, or practices of Day Kimball Hospital to protect the confidentiality, privacy, security, or accuracy of individually identifiable health information or employee's personal information. The privacy and security of employee records and protected health information, including financial records, will continue to be protected in accordance with existing applicable law and regulation as it may be amended from time to time.

III. DEFINITION(S):

A. Personal Information:

Personal information is defined as information capable of being associated with a particular individual through one or more identifiers, including, but not limited to a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, and does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

B. Covered Accounts:

Covered account means (i) any account that the Hospital offers or maintains primarily for personal, family, or household purposes, that involves multiple payments or transactions, including one or more deferred payments; and (ii) any other account the Hospital identifies as having a reasonably foreseeable risk to customers or to the safety and soundness of the Hospital from identity theft.

C. Identity Theft:

"Identity theft" means fraud committed using the identifying information of another person.

D. "Red Flags":

"Red flags" are those patterns, practices or specific activities that signal possible identity theft. Red Flags include, but are not limited to, the following:

1. Suspicious documents such as:

- identification cards or documents that appear to have been altered or forged, or contain information that is not consistent with existing records
- the photograph or physical description on identification cards or documents provided to Day Kimball Hospital is inconsistent with the appearance of (or information known about) the individual.

2. Suspicious personal identifying information, such as Social Security number in a range that does not correlate with date of birth, or invalid phone number or address that is not resolved with reasonable efforts to obtain accurate information.

3. Alerts from others (e.g., customer, identity theft victim, or law enforcement).

   The Identity Theft Red Flags Mitigation and Resolution Guidelines (Appendix A) identifies the Red Flags that would be most relevant to the Hospital.

   The list of Red Flags may be updated or supplemented in the form of a departmental procedure from time to time, and as more information becomes available to the health care industry with respect to medical identity theft.

IV. PROCEDURE:

A. Use of Personal Information: Personal information is only used to conduct Day Kimball Hospital's business in accordance with state and federal law.

B. Detection/Reporting:

1. Staff that suspect that a Red Flag has been implicated in relation to an individual with which Day Kimball Hospital has a continuing relationship to obtain payment for services shall report such incident to his/her supervisor.

2. If the Red Flag cannot be reconciled after a preliminary review of available records, and review of additional information from medical records, comparison with other government-issued identification cards and/or documents, and after making reasonable attempts to obtain clarification from the patient, family, and/or responsible party, the attached form, (Attachment A) should be completed promptly ("Identity Theft – Report of Suspicious Conduct/Documents") and provided to the Corporate Compliance Officer or authorized designee.

3. Intentional Fraud: Any indication that a Day Kimball Hospital identification card, number and/or other eligibility information provided by or on behalf of an individual, in order to obtain coverage under commercial insurance plans, workers' compensation, automobile accident coverage, government programs or other third party payers, is intentionally provided under fraudulent circumstances and/or does not belong to the individual presenting for admission or care and treatment will be reported to the Corporate Compliance Officer or authorized designee immediately. The attached form, (Attachment A) ("Identity Theft – Report of Suspicious Conduct/Documents") should be completed and provided to the Corporate Compliance Officer or designee promptly.

4. Fiscal records related to the incident are retained in order to review the possible identity theft incident(s) until the matter is resolved. Fiscal records include, but are not limited to the following:

   a. demographic information collected from a patient or responsible person,
   b. any transactions related to payment for services and/or deferred payment plans,
   c. documents related to insurance coverage or eligibility for third party reimbursement (Medicare, Medicaid, etc.)

5. In order to facilitate detection of the Red Flags identified in Appendix A, (appropriate Hospital staff) will take the following steps to obtain and verify the identity of the person:

   a. <u>New Patient Accounts</u>:

      1) Require identifying information, (e.g., full name, date of birth, address, government-issued ID, insurance card, etc.).
      2) When available, verify information with insurance company's information.
      3) Run a credit check.

   b. <u>Existing Accounts</u>:

      1) Verify validity of requests for changes of billing address.
      2) Verify identification of customers before giving out any personal information.

   c. <u>Preventing and Mitigating Identity Theft</u>:

      In order to prevent and mitigate the effects of Identity Theft, staff will follow the appropriate steps identified in the attached Identity Theft Red Flags Mitigation and Resolution Procedures (Appendix A).

   d. <u>Updating Program</u>:

      The Day Kimball Hospital Red Flags Identity Theft Program, and/or related department procedures or guidance, will be updated as needed to reflect changing risks, alerts from law enforcement, industry practices, and changes in methods related to preventing and detecting medical identity theft.

e. Service Provider Arrangements:

The hospital will require, by contract, that service providers that perform activities in connection with Covered Accounts have policies and procedures in place designed to detect, prevent, and mitigate the risk of Identity Theft with regard to the Covered Accounts.

f. Storage of and Access to Personal Information:

1) Storage: All documents containing personal information shall be stored in locked or secured areas. All computer applications containing Social Security numbers shall be maintained on secured, authorized-access computer stations only.
2) Access: Only persons who have a legitimate business reason will have access to Social Security numbers; such access will be granted through department heads responsible for functions with reporting or transporting of such data responsibilities. Department heads and employees granted such access must take all necessary precautions to ensure the integrity of records that include such numbers when the records are not being used.

g. Destruction of Personal Information:

Records that include personal information, including Social Security numbers, will be maintained in accordance with federal and state laws. When such documents are released for destruction, the physical records will be destroyed by shredding and electronic records shall be erased or the equipment on which such electronic records are stored should be physically destroyed so such records are unreadable.

Any individual who is found, after appropriate investigation, to have violated the provision of this policy, will be subject to disciplinary action, up to and including termination.

REFERENCES: FTC regulations – 16 C.F.R. § 681.2
CGS § 52-571h; CGS § 53a-129a *et seq*
Connecticut Public Act no. 06-167 "An Act Concerning the Confidentiality of Social Security Numbers"

CT General Statute § 53a-129a: "A person commits identity theft when such person intentionally obtains personal identifying information of another person without the authorization of such other person and uses that information to obtain or attempt to obtain money, credit, goods, services, property or medical information in the name of such other person without the consent of such other person."

Appendix A

Relevant Identity Theft Red Flags Mitigation and Resolution Guidelines

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	RESOLUTION OF RED FLAG *[ONLY SUGGESTIONS]*
Documents provided for identification appear to have been altered or forged.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the patient. For example, there is a lack of correlation between the Social Security Number (SSN) range and date of birth.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
The SSN provided is the same as that submitted by other persons opening an account or other customers.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
Patient has an insurance number but never produces an insurance card or other physical documentation of insurance.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient (*e.g.*, inconsistent blood type).	Investigate complaint, interview individuals as appropriate, review previous files for potential inaccurate records. Items to consider include: blood type, age, race, and other physical descriptions may be evidence of medical identity theft.	Depending on the inconsistency and review of previous file, either delay/do not open a new covered account, or reevaluate services. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Complaint/inquiry from an individual based on receipt of: -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 patronized - a notice of insurance benefits (or Explanation of Benefits) for health services never received.	Investigate complaint, interview individuals as appropriate	Reevaluate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	RESOLUTION OF RED FLAG *[ONLY SUGGESTIONS]*
Complaint/inquiry from a patient about information added to a credit report by a health care provider or insurer.	Investigate complaint, interview individuals as appropriate	Reevaluate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Complaint or question from a patient about the receipt of a collection notice from a bill collector.	Investigate complaint, interview individuals as appropriate	Reevaluate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Patient or insurance company report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.	Investigate complaint, interview individuals as appropriate	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's covered account.	Skip-tracing procedures are used to find the patient's current mailing address.	Patient is found and contact information is updated.
Hospital is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.	Investigation to determine if billing was made fraudulently.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary. Notify law enforcement as appropriate.

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	RESOLUTION OF RED FLAG *[ONLY SUGGESTIONS]*
		If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Personal identifying information provided by the patient is associated with known fraudulent activity as indicated by internal or third-party sources used by the Hospital. For example: - The address on an application is the same as the address provided on a fraudulent application; or - The phone number on an application is the same as the number provided on a fraudulent application.	Investigate complaint, interview individuals as appropriate	Reevaluate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.

Attachment A: Identity Theft – Report of Suspicious Conduct/Documents

Attachment A

Identity Theft Prevention Program
Identity Theft – Report of Suspicious Conduct/Documents

Complete information below – indicate "N/A" where appropriate

Person Completing Form – Name:_____

Unit/Dept.:_____Phone:_____Date:_____

Name of Patient:_____Med Rec #_____

Name(s) of Individual(s) Responsible for Patient's Account:_____

_____

Address(es) on file:_____

_____

_____

Describe Discrepancy and/or Suspicious Document(s) or Activity:

_____

_____

_____

_____

_____

_____

_____

_____

Attach copies of relevant document. **Retain all originals with file.**

Reference: HWP 12075