ADVENTIST HEALTH CARE, INC.
CORPORATE POLICY MANUAL

IDENTITY THEFT PROTECTION PROGRAM

Effective Date: 11/01/08	No: AHC 4.21
Cross Referenced:	Origin: OI
Reviewed:	Authority: SIO
Revised:	Page: 1 of 2

SCOPE:

This policy applies to:

1. All Adventist HealthCare, Inc. ("AHC"), entities including, but not limited to, hospitals, nursing homes, home health agencies, long-term care facilities, behavioral health operations, and physician practices; and

2. All employees, agents, contractors, vendors, physicians, volunteers, board members and business associates of Adventist HealthCare.

PURPOSE:

In keeping with our core values of respect, integrity, service, excellence and stewardship ("RISES"), and a commitment to conduct its business in an ethical and compliant manner, AHC has developed this policy to prevent the theft or misuse of patient names, identities, or other personal financial information.

POLICY:

1. General Requirements

A. Compliance with the Law: It is the policy of AHC to obey all federal and state laws, to develop policies & procedures to detect and prevent fraud, waste and abuse regarding payments from federal or state healthcare programs, and to provide protections for those who report actual or suspected wrongdoing.

B. Red Flags Rule: The FTC "Red Flags Rule" requires "creditors" holding "covered accounts" to develop an identity theft prevention program. "Covered accounts" are those that a creditor maintains primarily for personal, family or household purposes and involve multiple transactions or payments. The term "creditor" applies to any organization that defers payment for services rendered. Under the Rule, AHC, as a creditor holding covered accounts, must develop an identity theft prevention program that includes reasonable policies and procedures for detecting or mitigating identity theft.

C. Identity Theft Protection Program:

1. Employees should be alert for the following "red flags" which may indicate potential identity theft:

   - Address or name discrepancies;
   - Information presented by individual does not match information on file;
   - Suspicious documents presented;
   - Complaint from a patient or law enforcement;
   - Photo ID that does not match the patient;
   - Social security number is different than one used on a previous visit;
   - Family or friends call the patient by a name different than what was provided by the patient at registration;

2. Employee's who believe identity theft has occurred should immediately contact their Supervisor and the Entity Chief Privacy Officer. The employee's Supervisor and/or Chief Privacy Officer will contact Security as needed to assist with the investigation or to report criminal activity to law enforcement officials. The Supervisor and/or Chief Privacy Officer will also facilitate steps to correct and/or prevent further harm to any individual whose identifying information was used unlawfully or inappropriately.

3. Do not refuse care to anyone because they do not have acceptable identification. Instead, provide the necessary care and ask the patient to bring appropriate documents **as soon as they can.**

4. Some departments, such as Admitting and Patient Financial Services, may have a higher risk of potential instances of identity theft, and should develop their own list of "red flags" in addition to any other procedures deemed necessary to detect and prevent identity theft.

Adventist HealthCare

Identity Theft Protection Program

Compliance with FTC "Red Flags" Rule





Approved by AHC Organizational Committee on: May 26th, 2009

Electronic Copy Available on AHC's OIP Web Site

Integrity…

We are above reproach in everything we do.

IDENTITY THEFT: CRIME OF THE 21ST CENTURY

Each year, millions of Americans have their identities stolen. The list of criminal uses for this stolen information is as endless as the damage done to the victim. Identity thieves may use the victims' information to steal money from bank accounts, apply for fraudulent credit cards, and even sell the victims information to other criminals. Indeed, identity theft has become the crime of the 21st Century.

To protect the public from identity theft, the Federal Trade Commission (FTC) issued the "Red Flags" regulation, which requires organizations to implement an Identity Theft Protection Program to prevent, detect, and mitigate obvious instances (i.e., "red flags") of identity theft.

Adventist HealthCare's Identity Theft Protection Program is designed to help Adventist HealthCare employees and physicians detect and report suspected identity theft so any impact to the patient can be mitigated, and process improvements implemented to prevent future occurrences of identity theft.

WHAT IS A "RED FLAG"?

Red Flags are suspicious activities, patterns, or "warning signs" indicating that an identity theft has occurred. Employees should be alert for the following "red flags" or "warning signs" which may indicate potential identity theft:

- Address or name discrepancies;
- Information presented by individual does not match information on file;
- Suspicious documents presented;
- Complaint from a patient or law enforcement;
- Photo ID that does not match the patient;
- Social security number is different than one used on a previous visit; and
- Family or friends call the patient by a name different than what was provided by the patient at registration.

A comprehensive list of potential red flags is attached as **Appendix A**. Some departments, such as Admitting and Patient Financial Services, may have a higher risk of potential instances of identity theft, and should develop their own list of "red flags" in addition to specific departmental procedures deemed necessary to detect and prevent identity theft.

Knowing the Right Thing to Do and Doing the Right Thing

DETECTING & REPORTING "RED FLAGS"

Employee's who believe identity theft has occurred should immediately contact their Supervisor and the Entity Chief Privacy Officer. A listing of all AHC Chief Privacy Officers is posted on the **OIP Web Site**.

Employees may also report the Red Flag by calling the toll-free **Integrity Hotline at 1-800-814-1434**. The hotline is available 24/7, and employees may remain anonymous if they wish. In addition, employees may use the anonymous electronic reporting form located on the **OIP Web Site**.

The employees' Supervisor and/or Chief Privacy Officer will contact Security as needed to assist with the investigation or to report criminal activity to law enforcement officials. The employees' Supervisor and/or Chief Privacy Officer will also facilitate steps to correct and/or prevent further harm to any individual whose identifying information was used unlawfully or inappropriately.

RESPONSE & MITIGATION OF "RED FLAGS"

Effectively responding to a detected "red flag" will vary depending on the facts and circumstances of the suspected identity theft. Below are "response options" that may be used by the Department Supervisor, the Chief Privacy Officer, or Security, to mitigate the situation:

- Modify current security levels or protections (e.g., change passwords, access levels, etc.);
- Close patient accounts that have been breached;
- Amend (or place a note in) the medical record (or patient account) to flag the incident and its resolution;
- Notify law enforcement agencies and/or third-party payers of the identity theft; and
- Notify the patient that an identity theft has occurred.

TRAINING & EDUCATION ON "RED FLAGS"

Employees are required to complete annual HIPAA Privacy & Security Training via Learning Suite, a computer-based education delivery platform. In addition to HIPAA, employees will also be required to complete a Learning Suite module on Adventist HealthCare's Identity Theft Protection Program.

Knowing the Right Thing to Do and Doing the Right Thing

WHERE TO FIND MORE INFORMATION ON "RED FLAGS"

The sites below are helpful references:

- AHC's Organizational Integrity Website, https://extranet.adventisthealthcare.com/OIP/Default.aspx
- AHC's Policy 4.21, Identity Theft Protection Program, https://intranet.adventisthealthcare.com/policiesandprocedures/Corporate/Organizational%20Integrity%20Program/AHC%204.21.pdf
- Fighting Fraud with the Red Flags Rule: A How-To Guide for Businesses, http://www2.ftc.gov/redflagsrule
- World Privacy Forum Medical Identity Theft, The Medical Identity Theft Information Page, http://www.worldprivacyforum.org/medicalidentitytheft.html
- World Privacy Forum Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers, September 24, 2008, http://www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf
- Privacy Rights Clearinghouse, http://www.privacyrights.org/identity.htm#FS

Integrity…

We are above reproach in everything we do.

Appendix A

List of "Red Flag" Indicators of Identity Theft

I) Suspicious Documents:

(a) Altered/forged ID
(b) Inconsistent photo/description
(c) Inconsistent ID information
(d) ID information that doesn't match what is on file(i.e., signature, etc)
(e) Altered or forged application

II) Suspicious Personal ID information:

(a) Personal ID info inconsistent with external information
(b) Personal ID info inconsistent with other provided info or info on file
(c) Personal ID info associated with known fraud
(d) Duplicate SSN
(e) Duplicate Medicaid Card
(f) Duplicate address or telephone no.
(g) Incomplete info
(h) Individual unable to authenticate via challenge questions

III) Suspicious Activity:

(a) New or replacement request shortly following address change
(b) Usage consistent with known fraud patterns
(c) Unusual usage, inconsistent with established patterns
(d) Mail returned despite continued confirmation of address
(e) Patient complains about receiving bill denying receipt of services

IV) Suspicious Medical Information:

(a) Individual presents Medical background inconsistent with existing
(b) Individual unaware of basic medical background information
(c) Medical record inconsistent with physical examination or with patient's account of medical history
(d) Patient or insurance company report that coverage for legitimate hospital stay is being denied because benefits have been depleted
(e) Patient denies information provided in Medical Record
(f) Lab (blood work, etc,) inconsistent with information in medical record (wrong blood type, etc.)
(g) Patient refuses to produce insurance card