Identity Theft Prevention Program-Red Flag Rules

ROWAN UNIVERSITY POLICY

Title: Identity Theft Prevention Program-Red Flag Rules
Subject: Corporate Compliance and Privacy
Policy No: CCP:2017:01
Applies: Rowan University School of Osteopathic Medicine (RowanSOM)
Issuing Authority: Dean, RowanSOM
Responsible Officer: Chief Audit, Compliance & Privacy Officer
Date Adopted: 03/20/2017
Last Revision: 03/20/2020
Last Reviewed: 03/20/2020

I. PURPOSE

The purpose of this policy is to ensure that the RowanSOM complies with the Federal Trade Commission' s (FTC) Identity Theft Rules under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act). These regulations are also known as the Red Flags Rule. Under this policy, RowanSOM shall design a program to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. This program shall mitigate the risks associated with identity theft and mitigate the effects of identity theft on RowanSOM, its employees, its students, its patients, its constituents and its customers. This policy also addresses the administration of Perkins Loans, Institutional Loans and the provision of an extended tuition payment plan.

II. ACCOUNTABILITY

Under the direction of the Dean, the Clinical Dean for Academic and Clinical Affairs, the General Counsel and the Chief Audit, Compliance & Privacy Officer shall ensure compliance with this policy. The Dean, and Chief Operating Officer of RowanSOM shall implement this policy.

III. APPLICABILITY

This policy applies to the schools and units of RowanSOM, to the RowanSOM Community which includes RowanSOM management, faculty, and other academic personnel, clinical staff, researchers, employees, contractors, agents and others associated with or supporting RowanSOM.

IV. DEFINITIONS

1. *Account*: a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:
    a. An extension of credit, such as services involving a deferred payment, e.g. patient accounts, Perkins Loans and Institutional Loans; and
    b. A deposit account.
2. *Covered Account*: the Red Flags Regulations define the term "covered account" to mean:
    a. "an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions" and

b. “any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers, or to the safety and soundness of the financial institution, or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.”
c. For the purposes of the RowanSOM’s Identity Theft Program, the term “covered account” is extended to include any RowanSOM account or database (financially based or otherwise) for which RowanSOM believes there is a reasonably foreseeable risk to the RowanSOM, faculty, staff, patients, constituents or customers from identity theft.

3. *Credit:* the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.
4. *Creditor:* any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. A RowanSOM example of a “creditor” is Patient Accounts.
5. *Customer:* any person with a covered account with a creditor. A RowanSOM example of a “customer” is a patient who has been afforded a patient payment plan.
6. *Financial Institution:* a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer.
7. *Identity Theft:* the act of: knowingly obtaining, possessing, buying, or using, the personal identifying information of another: (i) with the intent to commit any unlawful act including, but not limited to, obtaining or attempting to obtain credit, goods, services or medical information in the name of such other person; and (ii) (a) without the consent of such other person; or (b) without the lawful authority to obtain, possess, buy or use such identifying information.
8. *Theft of Services:* includes: (i) intentionally obtaining services by deception, fraud, coercion, false pretense or any other means to avoid payment for the services; and (ii) having control over the disposition of services to others, knowingly diverts those services to the person's own benefit or to the benefit of another not entitled thereto.
9. *Notice of address discrepancy:* a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. § 1681(c)(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency’s file for the consumer.
10. *Person:* a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
11. *Personal Identifying Information:* any information that is requested in conjunction with a covered account that may be used alone, or in conjunction with any other information, to identify a specific person, e.g., credit card account information, debit card information, bank account information and drivers’ license information, social security number, mother’s birth name, and date of birth.
12. *Red Flag:* a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. The FTC regulations provide a list of 26 common red flags; organizations may decide that some of these 26 are not applicable, and/or that other red flags are more useful.
13. *Service Provider:* a person that provides a service directly to the financial institution or creditor.
14. *Transaction Account:* a deposit or account on which the depositor or account holder is permitted to make withdrawals by a negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. Such term includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

V. REFERENCES

1. 45 C.F.R. § 164.512(f)(5) (HIPAA crime on premises); 42 C.F.R. § 2.12 (c)(5)(ii);
2. Fair and Accurate Credit Transactions Act and federal regulations 16 CFR § 681

VI. BACKGROUND

1. RowanSOM strives to prevent the intentional or inadvertent misuse of patient names, identities and medical records; to report criminal activity relating to identity theft and theft of services to appropriate

authorities; and to take steps to correct and prevent further harm to any person whose name or other identifying information is used unlawfully or inappropriately.

2. In response to the growing threats of identity theft in the United States, Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended a previous law, the Fair Credit Reporting Act (FCRA). This amendment to FCRA charged the Federal Trade Commission (FTC) and several other federal agencies with promulgating rules regarding identity theft. On November 7, 2007, the FTC, in conjunction with several other federal agencies, promulgated a set of final regulations known as the "Red Flags Rule". The Red Flags Rule became effective January 1, 2008, however, the FTC has deferred its enforcement of the rule pending limiting legislation in Senate. On December 18, 2010, the Red Flag Rule Program Clarification Act of 2010 was signed by the President of the United States which clarifies the type of creditor that must comply with the rule and limits the circumstances under which creditors are covered. These creditors must comply by December 31, 2010. The new law covers creditors who regularly, and in the ordinary course of business, meet one of three general criteria. They must:
    a. obtain or use consumer reports in connection with a credit transaction;
    b. furnish information to consumer reporting agencies in connection with a credit transaction; or
    c. advance funds to -- or on behalf of -- someone, except for funds for expenses incidental to a service provided by the creditor to that person.
3. The Red Flags Rule regulations require entities with accounts covered by the Red Flags Rule regulations, including universities, to develop and implement a written Identity Theft Prevention Program (hereinafter, the "Program" or the "Identity Theft Program") for combating identity theft in connection with certain accounts. The Program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft and enable the entity with covered accounts to:
    a. Identify relevant patterns, practices, and activities, dubbed "Red Flags", signaling possible identity theft and incorporate those Red Flags into the Program; Detect the Red Flags that the program incorporates;
    b. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
    c. Ensure the Program is updated periodically to reflect changes in risks.

VII. POLICY

This policy outlines the Identify Theft Prevention Program of RowanSOM which encompasses not only financial or credit accounts, but any RowanSOM account or database for which RowanSOM believes there is a reasonably foreseeable risk to RowanSOM, faculty, staff, patients, constituents or customers from identity theft.

RowanSOM will implement and maintain an Identify Theft Prevention Program to assure compliance with federal law and RowanSOM policies preventing, detecting and mitigating possible identity theft of its patients, customers, clients and its constituents.

All RowanSOM employees and individuals working on behalf of RowanSOM in any capacity (including Board members, medical staff, business associates, independent contractors, and volunteers) will conduct themselves and their activities in a manner so as to protect the sensitive information, such as personal identifying information that may be used to defraud or aid identity theft as required by federal law and in conformance with RowanSOM policies.

1. Requirements:
    a. RowanSOM's Identity Theft Prevention Program will consist of the following elements:
        i. a detailed policy that specifically addresses this identity theft prevention program that includes reasonable policies and procedures to detect or mitigate identity theft and enable RowanSOM to:
            1. Conduct a survey to identify and detect potential and relevant "Red Flags" (See FTC's examples of red flags, EXHIBIT A) and incorporate the results of the survey into the program.
            2. Respond appropriately to red flags to prevent and mitigate identity theft.

3. Identify the Process of Establishing a Covered Account - this generally happens automatically when a patient makes an appointment and information is collected as part of that registration process.
4. Maintain access control to covered account information.
5. Address credit card payments.
6. Establish training requirements of employees and vendors, and
7. Ensure the Program is updated periodically to reflect changes in risks.

b. RowanSOM is required to adopt detailed processes and procedures (refer to EXHIBIT B) that will address the following identity theft concerns:
   i. Refusal to provide or lack of identification.
   ii. Process to follow if there are signs of possible identity theft.
   iii. Process to follow when an employee reasonably believes identity theft has occurred or may be occurring; include in the process to notify the Compliance Officer to advise of the potential identity theft. (Refer to EXHIBIT C for sample form).
   iv. Process to follow when identity theft is alleged by a patient; include the process to notify the Compliance Officer to advise of the potential identity theft. (Refer to EXHIBIT D for sample letter).
   v. Process to follow when identity theft is suspected to have occurred (including notification to law enforcement, customers, patients, etc.). (Refer to EXHIBIT E for sample letter).
   vi. Appropriately responding to detected Red Flags.
   vii. Notification from law enforcement and customers, patients, etc., when identify theft is suspected or known to have occurred (Refer to EXHIBIT F for sample letter).
   viii. Coordinating with area health care providers.
   ix. Process for entering patient accounts affected by identity theft on hold.
   x. Prevention and mitigation of identity theft.
   xi. Recoveries from suspect.
   xii. Accounting for inappropriate disclosures of protected health information.
   xiii. When patient misidentification occurs. (Refer to EXHIBIT E).
   xiv. Documenting identity theft or patient misidentification.
   xv. Updating the policy and procedures

c. Education and Training
   i. The Chief Audit, Compliance & Privacy Officer, or designee, will provide general training to refresh the University workforce regarding the Identity Theft Prevention Program, policies and procedures and the Red Flags Rule regulatory requirements.
   ii. Training of appropriate staff as determined by the Dean, Chief Operations Officer & Chief Audit, Compliance & Privacy Officer.
   iii. The Department of Human Resources will ensure that all new members of the workforce partake in Identity Theft Prevention training within one month after the person joins the workforce.
   iv. School or Unit Privacy Liaisons will ensure retraining of the workforce whose functions are affected by a material change in the policies and procedures within a reasonable period after the change becomes effective.
   v. Training provided will be appropriately documented and the documentation will be maintained by RowanSOM Privacy Liaisons for a minimum of six (6) years or as specified by the New Jersey State Record Retention Schedule.

d. Updating The Program
   i. On an annual basis, as part of the Office of Compliance and Corporate Integrity's monitoring plan, the Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable. This review will include an assessment of which accounts and/or databases are covered by the Program, whether additional Red Flags need to be identified as part of the Program, whether training has been implemented, and whether training has been effective. In addition, the review will include an assessment of whether mitigating steps included in the Program remain appropriate, and/or whether additional steps need to be defined.

2. Responsibilities:
   a. The Vice President for Human Resources shall be responsible for communicating and enforcing the above policy as it relates to all RowanSOM employees.

b. The Chairpersons and Dean shall be responsible for communicating and enforcing the above policy as it relates to persons involved in patient contact.
c. The Clinical Affairs and Deans, shall be responsible for communicating and enforcing the above policy as it relates to persons involved in Faculty Practice and patient care. The Director of Purchasing or his or her successors shall be responsible for communicating and enforcing the above policy as it relates to contractors, agents, business associates, and others associated with or supporting RowanSOM.
d. Monitoring and Evaluation
    i. The Office of Compliance and Corporate Integrity Compliance Committee is the governing body for the evaluation and monitoring of the Identity Theft Prevention Program.
    ii. The program is subject to periodic audit.
    iii. The Chief Audit, Compliance & Privacy Officer and RowanSOM Chief Operating Officer (COO or their designee) will review the program at least annually.
    iv. The Chief Audit, Compliance & Privacy Officer and Investigators are responsible for investigating and reporting on allegations of non-compliance with RowanSOM Identity Theft Prevention Program policies.
    v. Privacy Liaisons, under the direction of the Chief Audit, Compliance & Privacy Officer, RowanSOM COO, and Investigators may be asked to conduct investigations of non-compliance with RowanSOM Identity Theft Prevention Program policies.

3. Documentation
    a. Documentation evidencing implementation of the Identify Theft Prevention Program, including complaints, training, sanctions, auditing, etc., will be maintained for a minimum of six (6) years or the time period specified by New Jersey State Retention Schedules, whichever is longer.
4. Enforcement:
    a. The Deans, Vice Presidents and Directors, with the assistance of the Department of Human Resources, will enforce the sanctions appropriately and consistently.

VIII. ATTACHMENT

1. Attachment A: FTC's Examples of Red Flags
2. Attachment B: Identity Theft Red Flag and Security Incident Reporting Procedure
3. Attachment C: Identity Alert Form
4. Attachment D: Sample Letter Regarding Patient Misidentification
5. Attachment E: Sample Letter Regarding Identity Theft
6. Attachment F: Sample Letter Regarding Identity Theft Report

ATTACHMENT A

FTC's Examples of Red Flags

	RISK FACTORS	**BILLING UNIT**	**Practice**
1.	Computer network intrusion		
2.	Hospital-based providers – data compromise by hospital employee		
3.	Hospital-based providers – data compromise by company employee		
4.	Practice – billing company data transfer – PAPER		
5.	Practice – billing company data transfer – ELECTRONIC		

6.	Billing company – practice data transfer – PAPER		
7.	Billing company – practice data transfer – ELECTRONIC		
8.	Patient credit card payments – employee theft of credit card information		
9.	Practice paper records (in practice office) – mishandled or stolen [may also be a HIPAA violation]		
10.	Practice paper records (billing company office) – mishandled or stolen [see above]		
11.	Patient telephone inquiry to practice – alleges services not theirs, provider unknown, etc.		
12.	Patient telephone inquiry to billing company – alleges services not theirs, provider unknown, etc.		
13.	Insurer inquiry to practice – insured address does not match their records		
14.	Insurer inquiry to billing company – insured address does not match their records		
15.	Patient statements – mail interception and/or theft reported		
16.	Mail to patient returned to the practice – “Addressee Unknown,” etc.		
17.	Mail to patient returned to the billing company – “Addressee Unknown,” etc.		
18.	Patient / Guarantor denies receipt of monthly statements/correspondence		
19.	Collection agency reports inconsistencies in address, SSN, phone #, employment, etc.		
20.	Patient and/or Guarantor SSN is already on file – under another name(s)		
21.	Patient and/or Guarantor phone number(s) match others on file @ different addresses		
22.	Calls to home phone number(s) supplied are answered by “wrong number” responses		
23.	Patient or Guarantor calls to report their identity has been compromised		
24.	Contact from Credit Bureau(s) about a patient who has reported identity theft		
25.	Contact from USPS Inspectors or the USPS OIG regarding identity theft		
26.	Suspicious activity within an on-line payment portal – hosted by the practice		

27.	Suspicious activity within an on-line payment portal – hosted by the billing company or vendor		
28.	Credit card / debit card payments are denied or voided due to identity discrepancies		

ATTACHMENT B

Identity Theft Red Flag and Security Incident Reporting Procedure

1. Purpose
    a. The purpose of the *Identify Theft Red Flag and Security Incident Reporting Procedure* is to provide information to assist individuals in (1) detecting, preventing, and mitigating identity theft in connection with the opening of a "covered account" or any existing "covered account" or who believe that a security incident has occurred and (2) reporting a security incident.
2. Background
    a. Security Incident
        i. The American Recovery and Reinvestment Act (ARRA) requires that any organization that owns computerized data that includes personal information shall disclosure any breach of security of the system following discovery or notification of the breach in the security of the system to whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
    b. Red Flag Rules
        i. In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACT Act) which required the Federal Trade Commission (FTC) to issue regulations requiring "creditors" to adopt policies and procedures to prevent identify theft.
        ii. In 2007, the Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule. The rule requires "financial institutions" and "creditors" holding "covered accounts" to develop and implement a written identity theft prevention program designed to identify, detect and respond to "Red Flags."
        iii. The Red Flag Rule has been implemented by the Federal Trade Commission (FTC) on August 1, 2009.
3. Definitions
    a. Covered Account
    A covered account is a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a fee installment payment plan.
    b. Creditor
    A creditor is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit. Examples of activities that indicate a college or university is a "creditor" are:
        i. Offering institutional loans to faculty or staff;
        ii. Offering a plan for payment of patient services rather than requiring full payment
    c. Personal Information
    This information includes an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: Social Security Number, driver's license, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
    d. Red Flag
    A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

e. Security Incident
A collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

4. Identification of Red Flags
   a. Broad categories of "Red Flags" include the following:
      i. *Alerts* – alerts, notifications, or warnings from a consumer reporting agency including fraud alerts, credit freezes, or official notice of address discrepancies.
      ii. *Suspicious Documents* – such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut up, re-assembled and photocopied.
      iii. *Suspicious Personal Identifying Information* – such as discrepancies in address, Social Security Number, or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; personal information of others already on file; and/or failure to provide all required information.
      iv. *Unusual Use or Suspicious Account Activity* –such as material changes in payment patterns, notification that the account holder is not receiving mailed statement, or that the account has unauthorized charges;
      v. *Notice from Others Indicating Possible Identify Theft*–such as the institution receiving notice from a victim of identity theft, law enforcement, or another account holder reports that a fraudulent account was opened.
5. Detection of Red Flags
   a. Detection of Red Flags in connection with the opening of covered accounts as well as existing covered accounts can be made through such methods as:
      i. Obtaining and verifying identity;
      ii. Authenticating employees or patients;
      iii. Monitoring transactions
   b. A data security incident that results in unauthorized access to an employee's or patient's account record or a notice that an employee or patient has provided information related to a covered account to someone fraudulently claiming to represent RowanSOM or to a fraudulent web site may heighten the risk of identity theft and should be considered Red Flags.
6. Response to Red Flags
   a. If an employee or patient detects fraudulent activity (a red flag) or if an employee or patient claims to be a victim of identity theft, RowanSOM will respond to and investigate the situation. If the fraudulent activity involves protected health information (PHI) covered under the HIPAA security standards, RowanSOM will also apply its existing HIPAA and ARRA security policies and procedures to the response. If potentially fraudulent activity (a red flag) is detected by an employee or patient of RowanSOM:
      i. The employee/patient should gather all documentation and report the incident to his or her designated compliance officer.
      ii. The compliance officer will determine whether the activity is fraudulent or authentic based upon the evidence presented.
      iii. If the activity is determined to be fraudulent, then RowanSOM should take immediate action. Actions may include:
         1. Cancel the transaction
         2. Notify appropriate enforcement agencies
         3. Notify the affected employee or patient
         4. Notify affected physician(s)
   b. If an employee or patient claims to be a victim of identity theft:
      i. the employee/patient should be encouraged to file a police report for identity theft if he/she has not done so already
      ii. the employee/patient patient should be encouraged to complete the ***ID Theft Affidavit*** dev eloped by the FTC, along with supporting documentation **www.ftc.gov/bcp/edu /resources/forms/affidavit.pdf**.
   c. If following investigation, it appears that the employee/patient has been a victim of identity theft, RowanSOM will promptly consider what further remedial action/notifications may be needed under the circumstances.
7. Security Incident Reporting

    a. An employee who believes that a security incident has occurred, shall immediately notify their designated compliance officer or call the hotline at 1-855-431-9967.
    b. Service Providers
8. RowanSOM remains responsible for compliance with the Red Flags Rule even if it outsourced operations to a third party service provider. The written agreement between RowanSOM and the third party service provider shall require the third party to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities. The written agreement must also indicate whether the service provider is responsible for notifying only RowanSOM of the detection of a Red Flag or if the service provider is responsible for implementing appropriate steps to prevent or mitigate identify theft.
9. Training
    a. All employees who process any information related to a covered account shall receive training following appointment on the procedures outlined in this document. Refresher training may be provided annually.
10. **References:**
    a. **Fair and Accurate Credit Transactions Act of 2003 (FACTA)**
    b. American Medical Association

ATTACHMENT C

IDENTITY ALERT FORM

This form should be completed by the hospital or other facility personnel when the identity of a patient is questioned, either because of identity theft or patient misidentification.

Form completed by: _____

Date/Time: _____

Title: _____

Department: _____

Patient presented to facility using the following information:

Name: _____

Phone: _____

Address: _____

_____

SS#: _____

DOB: _____

Date/ Time: _____

Presenting Complaint: _____
_____

_____
_____

_____
_____

_____
_____

Existing MR # Used: _____ New MR #: _____ I Created:
_____

Account No. Assigned: _____ Consent Form Signature:
_____

Insurance Information Presented (specify if Medicaid, Medicare, or other governmental programs):
_____

_____
_____

_____
_____

Was the health information of any other patient provided to this individual? Does the hospital/facility need to account for the disclosures.

Name of "other"
patient: _____

Other information (who discovered discrepancy; was Security called, was photo secured, etc.):

_____
_____

_____
_____

_____
_____

List all involved staff members:
_____

Based on investigation, the correct patient is:

Name: _____ Phone: _____

Address: _____ _____

SS#: _____DOB: _____

Reason: _____ _____

_____ _____

_____ _____

PLEASE ATTACH A COPY OF THE RELEVANT PHOTO ID AND FORWARD THE COMPLETED FORM TO THE FACILITY'S PRIVACY OFFICER; REGISTRATION DIRECTOR; SECURITY DIRECTOR; PATIENT ACCOUNT DIRECTOR; AND THE COMPLIANCE OFFICER.

ATTACHMENT D

Identity Theft/Patient Misidentification Policy

Sample Letter Regarding Patient Misidentification

[Date]

[Patient Name]

[Patient Address]

[Patient Address]

Dear [Mr. ___/ Ms. ____]:

This letter is [to inform you of / in response to your report of] an erroneous use of your name or identifying information at [Name of entity] ("Entity") and to provide you with information to assist you in preventing this incident from affecting your medical care.

[Explain factual situation and describe how records became commingled.]

The integrity of your medical record is very important, and your record should only reflect your health history and medical items services provided to you. For example, if the blood type is of another person is listed in

your record, you could be given the wrong type of blood in an emergency. Therefore, **for your health and safety,** it is very important that your medical records do not contain information about another person. **We request your assistance in ensuring that our records about you are correct.**

We have removed from your medical record information relating to care given on _____ because [we have determined/you have indicated] you did not receive services at this hospital/site on those dates. After removing that information, your medical record shows the following visits:

Date of Visit	Reason for Visit
[insert]	

If someone other than you made any of the above visits, or you do not remember one or more of these visits, please contact us immediately. **You can review your entire medical record by visiting this facility's Medical Records Department, and we encourage you to do so.** In addition to making sure your medical record with this facility is accurate, we also encourage you to check the accuracy of your records with other health care providers and your health insurance plan(s).

[Based on the information we have received relating to the use of your name and other identifying information on _____, this facility will not bill you or your insurer for the services it provided on _____. We are in the process of correcting your account with your health insurer. If you receive a bill or insurance statement relating to a visit to this facility by someone other than you, please let us know as soon as possible.] We also recommend that you carefully monitor explanations of benefits (EOBs) received from your health insurer. If you receive an EOB or bill for health care you do not remember obtaining, immediately contact your insurer and the health care provider who furnished the services.

We hope this letter is helpful. If there is any other way the entity can assist you, or should you have any questions, please do not hesitate to contact me.

Sincerely,

_____

Privacy Officer

[Facility]

[Telephone number]

ATTACHMENT E

Identity Theft/Patient Misidentification Policy

Sample Letter Regarding Identity Theft

[Date]

BY CERTIFIED MAIL, RETURN RECEIPT REQUESTED

[Patient Name]

[Patient Address]

[Patient Address]

Re: **Suspected Identity Theft**

Dear _____:

This letter addresses the unauthorized use of your name and other personal information at _____ on _____. [Explain factual situation and describe compromise of information in detail (e.g., how it happened; information disclosed; what actions have been taken to remedy situation, etc.). Include the statement that, "We have reported this incident to _____ (name law enforcement officer) at the ____ [local law enforcement agency], who can be reached at _____. We also have placed an alert on your account at this facility in an effort to prevent further misuse of your identity."]

"Medical identity theft" is very serious because, in addition to causing financial problems, identity theft can lead to inappropriate care when incorrect information is included in a patient's medical record. For example, if the blood type of a person who misused your health insurance information is listed in your record, you could be given the wrong type of blood in an emergency. If you believe you are the victim of medical identity theft, you should ask to review and make appropriate corrections to your medical record so that you receive appropriate care. Therefore, **for your health and safety,** it is very important that your medical records do not contain information about another person. **We request your assistance in ensuring that our records about you are correct.**

We have removed from your medical record information relating to care given on _____ because [we have determined/you have indicated] you did not receive services at this facility on those dates. After removing that information, your medical record shows the following visits:

Date of Visit	Reason for Visit
[insert]	

If someone other than you made any of the above visits, or you do not remember one or more of these visits, please contact us immediately. **You can review your entire medical record by visiting this facility's Medical Records Department, and we encourage you to do so.** In addition to making sure your medical record with this facility is accurate, we also encourage you to check the accuracy of your records with other health care providers and your health insurance plan(s).

[Based on the information we have received relating to the improper use of your name and other identifying information on _____, this facility will not bill you or your insurer for the services it provided on _____. We are in the process of correcting your account with your health insurer. If you receive a bill or insurance statement relating to a visit to this facility by someone other than you, please let us know as soon as possible.] We also recommend that you carefully monitor explanations of benefits (EOBs) received from your health insurer to determine if any other person has used your identity to obtain health care. If you receive an EOB or bill for health care you do not remember obtaining, immediately contact your insurer and the health care provider who furnished the services.

Given the possibility that your personal information may be further misused, we recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you and verify your identity before they open any new accounts or change existing accounts. You can call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. **All three credit reports will be sent to you, free of charge, for your review.**

Equifax	Experian	TransUnionCorp
800-525-6285	888-397-3742	800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, you should continue monitoring your credit reports carefully to be certain there have been no unauthorized transactions made or new accounts opened in your name. Victim information sometimes is held for use or shared among a group of **thieves** at different times. Checking your credit reports periodically can help you spot problems and address them quickly. You are entitled under federal law to get one free comprehensive disclosure of all the information in your credit file from each of the three national credit bureaus listed about once every twelve months. You may request your free annual credit report by visiting http://AnnualCreditReport.com or by calling (877)FACTACT.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, immediately notify the credit bureaus. If you believe an unauthorized account has been opened in your name, immediately contact the financial institution that holds the account. You should also file a police report. Ask for a copy of the police report because many creditors want the information it contains to absolve you of the fraudulent debts. You should also file a complaint with the FTC at www.consumer.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. You may want to visit the FTC's website at http://www.ftc.gov/bcp/edu/microsites/idtheft/, which has information to help individuals guard against and deal with identity theft, and you may want to review the information in the FTC's publication, "Take Charge: Fighting Back Against Identity Theft." You can call 1-877-438-4338 to request a free copy.

We encourage you to report any helpful information to _____ [investigating law enforcement officer] at the ____ [local law enforcement agency]. We also encourage you to alert other area hospitals and health care providers that your identifying information is being used in a fraudulent manner. If we can be of further assistance, please contact me at the number listed below.

Sincerely,

_____

Unit Designee

[Facility]

[Telephone number]

ATTACHMENT F

Identity Theft/Patient Misidentification Policy

Sample Letter regarding Identity Theft Report

[**Date]**

[Patient Name]

[Patient Address]

[Patient Address]

Re: Identity Theft Report Made on_____ **[date]**

RESPONSE REQUIRED

Dear _____:

This letter responds to your report that a person used your name, insurance information, or other personal information to obtain health care items or services at this facility. Please follow the instructions in this letter so that we can help you address this problem.

After reading the instructions for the enclosed Identity Theft Affidavit, complete the Identity Theft Affidavit (also available at http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf), including all details of the identity theft incident that you know. Make copies of the required documentation (e.g., photo identification; police report regarding the incident, etc.) and attach them to your affidavit. Sign the affidavit, then, have the affidavit notarized or witnessed by two people who are not members of your family. **Return the completed signed affidavit and accompanying documentation to this office within two weeks from the date of this letter so this facility can take the necessary steps to correct your medical record and patient account**.

"Medical identity theft" is very serious because, in addition to causing financial problems, identity theft can lead to inappropriate care when incorrect information is included in a patient's medical record. For example, if the blood type of a person who misused your information is listed in your record, you could be given the wrong type of blood in an emergency. Once we receive your completed and signed affidavit, and appropriate supporting documentation, our Health Information Management and Patient Accounts office will work with you to make necessary corrections to your medical record and patient accounts. **In the meantime, should you need to visit this facility or any other health care provider, you should let the provider know that the information in your medical record may be incorrect because your identity has been used to obtain health care items or services fraudulently.**

We encourage you to alert other area hospitals and health care providers that your identifying information is being used in a fraudulent manner because identity thieves often obtain services and items from more than one health care provider. You may also want to visit the FTC's website at http://www.ftc.gov/bcp/edu/microsites/idtheft/, which has information to help individuals guard against and deal with identity theft, and you may want to review the information in the FTC's publication, "Take Charge: Fighting Back Against Identity Theft." You can call 1-877-438-4338 to request a free copy.

Sincerely,

_____

_____

Enclosure (FTC Identity Theft Affidavit)