IDENTITY THEFT/RED FLAG RULES

KEYWORDS: Theft, intentionally misrepresenting, fictitious, identities, identity, phony, misuse, unlawfully and inappropriate.

PURPOSE: To describe the measures to be followed when health care is obtained under a fictitious name or in another person's name. This includes situations when a person intentionally misrepresents himself/herself and when a person gives his/her real name, but the facility accesses the wrong medical record so that the medical records of two patients are commingled.

SCOPE: All St. Joseph's Healthcare System facilities

LEGAL/REGULATORY CITES: 16 CFR Part 681,72

DEFINITIONS: Identity theft means 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.

POLICY: St. Joseph's Healthcare System (SJHS) facilities strive 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/or prevent further harm to any person whose name or other identifying information is used unlawfully or inappropriately.

PROCEDURE:

1. Request Identification at Registration/Intake Points. SJHS emergency departments and all other registration/intake areas should review and include in each patient's file a photo ID issued by a local, state, or federal government agency (e.g., a driver's license; passport; military ID, etc.). In the event the patient does not have photo ID, ask for two forms of non-photo ID, one of which has been issued by a state or federal agency (e.g....Social Security, card and a utility bill or company or school identification). When the patient is under 18 or if the patient is unable due to their condition to produce identification, the responsible party's identification shall be requested. Each time a patient visits, check whether the identification provided is valid, copy the identification provided, and match any photo to the patient/responsible party. During the registration process, if an identity alert flag appears in the SJHS Master Patient Index (MPI) call the Registration Supervisor or the Privacy/Compliance Officer for resolution.

A. Emergency Care—NO DELAY. Providing identification is not a condition for obtaining emergency care. The process of confirming a patient's identity must never delay the provision of an appropriate medical screening examination or necessary stabilizing treatment for emergency medical conditions.

B. Responding to Questions. If asked the reason for the identifying procedures, explain that the procedures are "for patient protection to prevent identity theft and theft of services." Politely remind questioners this is the same process used to cash a check, make a large credit card purchase, or board a plane.

C. Refusal to Provide or Lack of Identification. No one should be refused care because they do not have acceptable identification with them. Patients should be asked to bring appropriate documents to their next visit.

2. Signs of Possible Identity Theft. Employees should be alert for cases of possible identity theft. Potential signs of identity theft include: (1) any patient appearing and giving an identity that has been flagged in SJHS's MPI or Identity Theft Database, (2) a patient providing photo ID that does not match the patient, (3) a patient giving a social security number different than one used on a previous visit, (4) a patient giving information that conflicts with information in the patient's file or received from third parties, such as insurance companies, and (5) family members, friends calling the patient by a name different than that provided by the patient at registration. If an employee reasonably believes identity theft has occurred or may be occurring, immediately notify the Registration Supervisor or the Privacy/Compliance Officer. The Registration Supervisor/ Privacy/Compliance Officer will involve Security on an as-needed basis (e.g., to perform background checks, to contact the person believed to be a victim of the identity theft, and if medical circumstances allow to interview the patient, etc.) and notify General Counsel.

3. When Identity Theft Is Alleged by a Patient. Advise the patient to report the identity theft incident to law enforcement and indicate that paperwork will be forwarded for the patient to complete. The Privacy/Compliance Officer shall complete and send the letter attached as Exhibit A to the patient with a copy of the Federal Trade Commission (FTC) Identity Theft affidavit, attached hereto as Exhibit B, also available at http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf. Unless there is actual knowledge that identity theft has occurred at an SJHS facility, the facility must receive a properly completed and signed FTC Identity Theft Affidavit before correcting medical or payment records or proceeding with other victim assistance steps under this policy. Once an FTC Identify Theft Affidavit supports the identity theft allegation, the facility must flag the account of the patient alleging identity theft so that registration and medical personnel are alert to the issue that the medical record may contain inaccurate information about the patient. The facility then can proceed with the remainder of the steps set out in this policy.

4. When Identity Theft Occurs. If a person obtains or uses the personal identifying information of another to obtain (or to attempt to obtain) medical services or information in the name of such other person, the facility shall take the following steps:

A. Notifications. When identity theft is reasonably suspected or is known by an employee to have occurred (e.g., by receipt of a properly completed and signed FTC Identity

Theft Affidavit), the employee must immediately complete the Identity Alert reporting form attached as Exhibit C and route copies to the Privacy/Compliance Officer, Medical Records/Health Information Management Director (HIM), Security Director, Registration Director, Patient Account Director, and Legal Affairs. Attach a copy of the relevant photo ID if available. If the incident occurs on a weekend, reporting should occur the next business day. The Privacy/Compliance Officer will review and make a recommendation on the findings and external reporting and notification decisions. External notification and reporting will occur only as directed by the General Counsel.

i. Reporting Medicaid Fraud. When there is actual knowledge of Medicaid fraud (e.g., a patient uses another person's Medicaid information to obtain medical care), the fraud

ii. must be reported immediately to the Medicaid OIG: 1-866-633-6585.

ii. Mail Theft. For incidents involving mail theft, the U.S. Postal Inspection Service will be contacted.

iii. Security Breach. If the identity theft involves unauthorized access of unencrypted *computerized* data containing a person's first name or first initial and last name and

(1) a social security number, (2) driver's license number, or (3) financial account number (including a credit or debit card number) in combination with any required security

(2) code, access code, or password that would permit access to an individual's financial account, the Privacy/Compliance Officer, after discussion with the General Counsel,

(3) will direct reporting to the individual whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person in accordance

(4) with New Jersey and federal law. Such reporting will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.

iv. Coordinating with Area Health Care Providers. The victim's written authorization generally will be obtained prior to alerting non-SJHS health care providers about the possibility of identity theft in connection with the victim's identifying information. (*See* SJHS Policy # 1902 Authorization for the Release of Medical Records). However, in the event circumstances indicate that the identity thief may imminently use the victim's information to defraud a non-SJHS health care provider (e.g., identity thief is "shopping" area emergency departments for medication) and such circumstances do not allow enough time to obtain the victim's written authorization to disclose the victim's name and address to the non-SJHS provider to prevent further fraudulent activity in connection with the victim's identifying information, after consulting with the General Counsel the Privacy/Compliance Officer may disclose (or direct disclosure) information about the identity theft victim to a non-SJHS provider to allow the unrelated provider to determine whether it has an existing or past relationship with the victim. The information disclosed shall be limited to the minimum necessary to determine whether the victim has an existing or past relationship with the area health care provider (e.g., victim's name and address; photograph of identity theft suspect). If the non-SJHS provider confirms it has an existing or past relationship with the victim, the minimum necessary information regarding the identity theft incident may be disclosed so that the provider is alert to the potential for fraudulent activity related to the victim's identifying information. In the event the identity theft victim does not have an existing or past relationship with the non-SJHS provider,

the victim's written authorization must be obtained prior to releasing any identifying information about the victim to a non-SJHS provider.

B. Accounts on Hold. The Patient Accounts Director will put all patient accounts affected by the identity theft on hold pending the outcome of the investigation.

C. Security Department; Reports to Law Enforcement; Reporting Medicaid Fraud. The SJHS Security Department will provide any necessary assistance with determining the identity of the patient and provide feedback to the Registration Director, Patient Accounts Director, and the Privacy/Compliance Officer. If the Privacy/Compliance Officer together with General Counsel believe in good faith that identity theft or theft of services has occurred on SJHS's premises, and the value of the services in question exceeds or may exceed $500, the Privacy/Compliance Officer will instruct SJHS's Security Department to report the incident to the Prosecutor's Office in Passaic County and, depending on which facility, the Paterson or Wayne Police Department. In order to facilitate reporting and efficient prosecution of identity theft crimes, the Privacy/Compliance Officer shall prepare a summary of the information that SJHS believes in good faith constitutes evidence of criminal conduct that occurred on the SJHS's premises (e.g., information provided by the victim and the suspect; any fingerprint, photo, and copies of security films taken of the suspect; a statement of the value of services obtained by the suspect, etc.). The Security Department will make reasonable efforts to limit the disclosure of protected health information to the minimum necessary to report the suspected identity theft, and the information disclosed will not directly or indirectly identify any patient as a mental health services recipient. The Security Department must obtain the investigating officer's name and phone number consult with law enforcement about the timing and the content of any victim notification (to ensure notification does not impede a law enforcement investigation), and explain that the investigating officer's name and phone number will be shared with the identity theft victim in any victim notification.

D. Notifying Victims of Identity Theft When the Patient Does Not Know Identity Theft Has Occurred. After consultation with law enforcement about the timing and the content of any victim notification (to ensure notification does not impede a law enforcement investigation), victims of identity theft will be notified by the Privacy/Compliance Officer after discussion with the General Counsel. The letter attached to this Policy as Exhibit D shall be used to notify a victim of identity theft. Victims of identity theft should be encouraged to cooperate with law enforcement in identifying and prosecuting the suspected identity thief. Encourage the victim to complete the FTC Identity Theft Affidavit attached hereto as Exhibit B and available at http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf.

E. Correcting Medical and Payment Records of Identity Theft Victims; Flagging; Verification and Releasing Bill Hold. To ensure that (1) inaccurate health information is not inadvertently relied upon in treating a patient, (2) a patient or a third-party payer is not billed for services the patient did not receive, and (3) patient health information is protected from inappropriate disclosure, patient medical and payment records must be corrected when a case of identity theft occurs.

i. Medical Records. After appropriate consultation with and input from the patient (whose identity has been properly verified and documented, including through receipt of a properly completed FTC Identity Theft Affidavit) and appropriate clinical personnel, the HIM department will make appropriate corrections to the patient's medical record to be certain the record contains

correct entries only (e.g.,by transferring visit from incorrect MPI record to appropriate MPI record). Corrections shall be made in accordance with the SJHS's Administrative Policy # 1903, *Amendment of Health Information*. A detailed explanation of the corrections shall be generated by SJHS and verified by the patient. Pursuant to SJHS HIPAA Policies, the HIM department may need to send amended information to persons who have received incorrect or incomplete information. The HIM department shall remove all related documents from the permanent record and replace them with appropriately revised documents. A notation of this amendment shall be made in the permanent record and the original documents sent to the Privacy/Compliance Officer for inclusion in the case file. The patient's verification of the corrected medical record shall be documented and included as part of the case file forwarded to the Privacy/Compliance Officer.

ii. Payment Records. After appropriate consultation with and input from the patient (whose identity has been properly verified and documented, including through receipt of a properly completed FTC Identity Theft Affidavit), the Patient Accounts department will make appropriate corrections to the patient's billing information, inform and provide documentation to any third-party payer affected by the adjustments, and make any necessary repayments to ensure that the patient and the payer pay only for services actually provided to the patient. Corrections shall be made in accordance with the SJHS's billing record corrections procedures and SJHS Administrative Policy # 1903, *Amendment of Health Information*. A detailed explanation of the corrections shall be generated by SJHS and verified by the patient. The patient's verification of the corrected billing records shall be documented and included as part of the case file forwarded to the Compliance officer.

iii. Flagging. The Registration Director will add an MPI Alert Flag of "Identity issue/ call Security" to each MPI record

iv. Verification; Release of Hold. The Registration Director and/or the Patient Accounts Director will verify that all demographic and insurance information is correct after the visit is transferred to the appropriate MPI record and will ensure that all related documents are removed from permanent records and replaced with appropriately revised documents. Once all medical and billing records have been corrected, the Registration Director and/or the Patient Accounts Director will release the bill hold and bill appropriately.

F. Assisting Identity Theft Victims

i. Copies of Records On Written Request. Identity theft victims are entitled to obtain a copy of the business transaction records maintained by the SJHS facility (or by others on the facility's behalf) relating to the identity theft free of charge. Business transaction records" may include billing and medical record information. The SJHS facility must provide these records within 30 days of receipt of the victim's written request. The facility also must provide these records to any law enforcement agency that the victim authorizes. Before providing such records, the facility must ask for proof of identity, which may be a government-issued ID card, the same type of information the identity thief used to access the patient's account, or the type of information the facility is currently requesting from patients, a police report (regarding the identity theft), and a completed FTC Identity Theft Affidavit available at

http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf, and attached hereto as Exhibit B). Document receipt of and copy all such information.

The SJHS facility may refuse to provide business transaction records if it is determined in good faith that: (i) the true identity of the person asking for the information cannot be verified; (ii) the request for the information is based on a misrepresentation; or (iii) state or federal law prohibits the facility from disclosing such information.

ii. Mitigation. The facility should mitigate, to the extent practicable, any harmful effect that is known to the facility as a result of unlawful use or disclosure of protected health information in connection with a case of identity theft.

G. Recoveries from Suspect. If a suspect is identified SJHS may bill the identity theft suspect for unlawfully obtained services and if SJHS has suffered an ascertainable loss (such as by providing services never paid for), SJHS may consider pursuing a civil claim. Consult with the General Counsel for further guidance.

H. Accounting for Disclosures. The Privacy/Compliance Officer should determine whether, as result of identity theft, protected health information was inappropriately disclosed. If protected health information was inappropriately disclosed, the HIM department must account for such disclosures in accordance with the SJHS Administrative Policy # 1919, *Accounting for Disclosures.*

I. Update Identity Theft Database. When identity theft is reasonably suspected, either the Registration Director or the Privacy/Compliance Officer must update the SJHS Identity Theft Database with the Identity Alert Form to include alerts on both the identity theft victim and any other name or identification provided by the suspect.

5. When Patient Misidentification Occurs. If it is determined that patient misidentification, but not identity theft, has occurred (as, for example, when a patient gives his or her real name, but the incorrect medical record is pulled up and the medical information of two patients is subsequently intermingled), the facility shall take the following steps:

A. Notifications. When patient misidentification has occurred, the employee discovering the misidentification must immediately complete the Identity Alert reporting form

B. attached as Exhibit C and route copies of the same to the Privacy/Compliance Officer, HIM Director, Security Director, Registration Director, Patient Account Director.

C. and the General Counsel. Attach a copy of the relevant photo ID if available. If the incident occurs on a weekend, reporting should occur the next business day.

D. The Privacy/Compliance Officer will review and make a recommendation on the findings and external reporting and notification decisions.

External notification and reporting will occur only as directed by the General Counsel.

i. Security Breach. If the identity theft involves unauthorized access of unencrypted *computerized* data containing a person's first name or first initial and last name and (1) a social security number, (2) driver's license number, or (3) financial account number (including a credit or debit card number) in combination with any required security code, access code, or password that would permit access to an individual's financial account, the Privacy/Compliance Officer, after discussion with the General Counsel will direct reporting to the individual whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person in accordance with New Jersey and federal law. Such reporting will be

made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.

B. Accounts on Hold. The Patient Accounts Director will put all patient accounts affected by the patient misidentification on hold pending the outcome of the investigation.

C. Notifying Affected Patients; Mitigation Efforts. The HIM Department will notify patients affected by patient misidentification. The letter attached to this Policy as Exhibit E shall be used to notify such patients. The facility should mitigate, to the extent practicable, any harmful effect that is known to the facility as a result of unlawful use or disclosure of protected health information in connection with a case of patient misidentification.

D. Correcting Medical and Payment Records; Verification; Release of Hold. To ensure that (1) inaccurate health information is not inadvertently relied upon in treating a patient, (2) a patient or a third party payer is not billed for services the patient did not receive, and (3) patient health information is protected from inappropriate disclosure, patient medical and payment records must be corrected when a case of patient misidentification occurs.

i. Medical Records: After appropriate consultation with and input from the patient (whose identity has been properly verified and documented) and appropriate clinical personnel, the HIM department will make appropriate corrections to the patient's medical record to be certain the record contains correct entries only (e.g.,by transferring visit from incorrect MPI record to appropriate MPI record). Corrections shall be made in accordance with SJHS Administrative Policy # 1903, *Amendment of Health Information*. A detailed explanation of the corrections shall be generated by SJHS and verified by the patient. Pursuant to SJHS HIPAA Policies, the HIM department may need to send amended information to persons who have received incorrect or incomplete information. The HIM department shall remove all related documents from the permanent record and replace them with appropriately revised documents. A notation of this amendment shall be made in the permanent record and the original documents sent to the Privacy/Compliance Officer for inclusion in the case file. The patient's verification of the corrected medical record shall be documented and included as part of the case file forwarded to the Privacy/Compliance Officer.

ii. Payment Records. After appropriate consultation with and input from the patient (whose identity has been properly verified and documented), the billing department will make appropriate corrections to the patient's billing information, inform and provide documentation to any third-party payer affected by the adjustments, and make any necessary repayments to ensure that the patient and the payer pay only for services actually provided to the patient. Corrections shall be made in accordance with SJHS's billing record corrections procedures and SJHS Administrative Policy # 1903, *Amendment of Health Information*. A detailed explanation of the corrections shall be generated by SJHS and verified by the patient. The patient's verification of the corrected billing records shall be documented and included as part of the case file forwarded to the Privacy/Compliance Officer**.**

iii. Verification; Release of Hold. The Registration Director and/or the Patient Accounts Director will verify that all demographic and insurance information is correct after the visit is transferred to the appropriate MPI record and will ensure that all related documents are removed from permanent record and replaced with appropriately revised documents. A notation of this amendment will be made in the file and copies of all amendments will be sent to the Privacy/Compliance Officer for the case file. Once all medical and billing records have been

corrected, the Registration Director and/or the Patient Accounts Director will release the bill hold and bill appropriately.

E. Accounting for Disclosures. The Privacy/Compliance Officer should determine whether, as result of patient misidentification, protected health information was inappropriately disclosed. If protected health information was inappropriately disclosed, the HIM department must account for such disclosures in accordance with the SJHS Administrative Policy # 1919, *Accounting for Disclosures*.

6. Documentation. A copy of all documentation concerning identity theft or patient misidentification must be provided to the Privacy/Compliance Officer who

shall maintain the permanent and complete file.

7. Checklists. Checklists for action items related to this policy are attached as Exhibit F.

8. Definitions. A. Identity theft means 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.

B. 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.

Signed Original in Administration

William McDonald
President/CEO

Exhibit A to Identity Theft/Patient Misidentification Policy

Letter regarding Identity Theft Report

{Date}

{Patient Name}

{Patient Address}

{Patient Address}

Re: Identity Theft Report Made on_____ {insert 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 St. Joseph's. We want to assist you and ask that you please follow the instructions in this letter so that we can

help you address this problem.

First, read 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. Second, make copies of the required documentation. (e.g., photo identification; police report regarding the incident, etc.) and attach them to your affidavit. Third, sign the affidavit, and have the affidavit notarized or witnessed by two people who are not members of your family. Fourth, 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 properly 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,

_____

Privacy/Compliance Officer

Enclosure (FTC Identity Theft Affidavit)

Exhibit B to Identity Theft/Patient Misidentification Policy

FTC ID Theft Affidavit

Instructions for Completing the ID theft Affidavit:

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened in your name that you didn't create the debt. The ID Theft Affidavit was developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) for this purpose. Importantly, this affidavit is only for use where a new account was opened in your name. If someone made unauthorized charges to an existing account, call the company for instructions.

While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it. If they do not accept the ID Theft Affidavit, ask them what information and/or documentation they require. You may not need the ID Theft Affidavit to absolve you of debt resulting from identity theft if you obtain an Identity Theft Report. We suggest you consider obtaining an Identity Theft Report where a new account was opened in your name. An Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit reports; (3) prevent a company from continuing to collect debts or selling the debt to others for collection; and (4) obtain an extended fraud alert. The ID Theft Affidavit may be required by a company in order for you to obtain applications or other transaction records related to the theft of your identity. These records may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement.

This affidavit has two parts:

• Part One — the ID Theft Affidavit — is where you report general information about yourself and the theft.

• Part Two — the Fraudulent Account Statement — is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account

Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them. Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation. Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly. When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide. Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit. If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

1. Any one of the nationwide consumer reporting companies to place a fraud alert on your credit card.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. The company you call is required to contact the other two, which will place an alert on their versions of your report also.

Equifax: 1-800-525-6285; www.equifax.com

Experian: 1-888-Experian (397-3742); www.experian.com

TransUnion: 1-800-680-7289; www.transunion.com

In addition, once you have placed a fraud alert, you're entitled to order one free credit report from each of the three consumer reporting companies, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

2. The security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close accounts. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card company's and banks in writing. Send your letters by certified mail, return receipt requested, so that you can document what the company received and when. Keep a file of your correspondence and enclosures. When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number, your phone number or a series of consecutive numbers
3. Your local police or the police in the community where the identity theft tool place. Provide a copy of your ID Theft Complaint filed with the FTC (see below), to be incorporated into the police report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, to try another jurisdiction like your state police. You can also check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check **www.naag.org** for a list of state Attorney Generals.
4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC also can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws that the FTC endorses. You can file a complaint online at www.consumer.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438- 4338); TTY: 1-866-653-4261; or write: Identity Theft Clearing House, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. When you file an ID Theft Complaint with the FTC online, you will be given the option to print a copy of your ID Theft Complaint. You should bring a copy of the printed ID Theft Complaint with you to the police to be incorporated into your police report. The ID Theft Complaint, in conjunction with the police report, can create an Identity Theft Repot that will help you recover more quickly. The ID Theft Complaint provides the supporting details necessary for an Identity Theft Report, which go beyond the details of a typical police report.

Name_____ Phone number
_____

ID THEFT AFFIDAVIT

(1) My full legal name is
_____

(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as
_____

(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is
_____

(day/month/year)

(4) My Social Security number is_____

(5) My driver's license or identification card state and number are
_____

(6) My current address is
_____
_____

City _____ State _____ Zip Code
_____

(7) I have lived at this address since
_____

(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was_____

City _____ State _____ Zip Code_____ _____
_____

(9) I lived at the address in Item 8 from _____ until
_____

VICTIM INFORMATION

(10) My daytime telephone number is (_____)_____

My evening telephone number is (_____) _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY.

SUBJECT: IDENTITY THEFT / RED FLAG RULES POLICY

Name_____ Phone number _____

How the Fraud Occurred

Check all that apply for items 11 – 17:

(11) □ I did not authorize anyone to use my name or personal information to seek the Money, credit, loans, goods or services described in this report.

(12) □ I did not receive any benefit, money, goods or services as a result of the events described in this report.

(13) □ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were □ stolen

□ lost on or about _____. (day/month/year)

(14) □ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____ _____

Name (if known) Name (if known)

_____ _____

Address (if known) Address (if known)

_____ _____

Phone number(s) (if known) Phone number(s) (if known)

_____ _____

Additional information (if known) Additional information (if known)

How the Fraud Occurred

(15) □ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) □ Additional comments: (For example, description of the fraud which documents or information were used or how the identity thief gained access to your information.)

_____
_____
_____
_____
_____
_____

(Attach additional pages as necessary.)

Name_____ Phone number
_____----------_____

(17) (check one) I □ am □ am not willing to assist in the prosecution of the person(s) who committed this fraud.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY.

(18) (check one) I □ am □ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I □ have □ have not reported the events described in this affidavit to the police or other law enforcement agency.

The police □ did □ did not write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

_____ _____

(Agency #1) (Officer/Agency personnel taking report)

_____ _____

(Date of report) (Report number, if any)

_____ _____

(Phone number) (email address, if any)

_____ _____

(Agency #2) (Officer/Agency personnel taking report)

_____ _____

(Date of report) (Report number, if any)

_____ _____

(Phone number) (email address, if any) Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies. (20) □ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence. (21) □ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

SUBJECT: IDENTITY THEFT/ RED FLAY RULES

Name_____ Phone number _____

(22) □ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith.

I also understand that this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within

their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. §1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

_____ _____

(signature) (date signed)

(Notary)

{Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.}

Witness:

_____ _____

(signature) (printed name)

_____ _____

(date) (telephone number)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Signature

Name_____ Phone number _____

Fraudulent Account Statement

• Make as many copies of this page as you need. Complete a separate page for each company you're notifying and only send it to that company. Include a copy of

your signed affidavit.

• List only the account(s) you're disputing with the company receiving this form. See the example below.

• If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/we reopened at your company in my name without my knowledge,

permission or authorization using my personal information or identifying documents:

Creditor Name/Address

_____

(the company that opened the account or provided the goods or services Account Number Type of unauthorized credit/goods/services provided by creditor (if known).

Date issued: _____or opened (if known)

Amount/Value Provided (the amount charged or the cost of goods/services Completing this Statement.

 During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address_____

Account number _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Exhibit C to Identity Theft/Patient Misidentification Policy

IDENTITY ALERT FORM

Hospital personnel should complete this form 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:_____

_____

Approximate Cost of Visit: _____

Existing MPI Used:_____ New MPI Created:_____

Account No. Assigned:_____ Consent Form Signature: _____

_____

Insurance Information Presented (specify if Was the health information of any other patient
Medicaid, Medicare, or other governmental provided to this individual (such that the
programs): _____ hospital/facility needs to account for such
_____ disclosures)?_____

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:_____

MPI: _____ Time:

_____

Reason:_____

_____

ATTACH A COPY OF THE RELEVANT PHOTO ID AND FORWARD THE COMPLETED FORM TO THE ST. JOSEPH'S HEALTHCARE SYSTEM PRIVACY/COMPLIANCE OFFICER; REGISTRATION DIRECTOR; SECURITY DIRECTOR; AND THE PATIENT ACCOUNT DIRECTOR ST. JOSEPH'S REGIONAL MEDICAL CENTER

Exhibit D to Identity Theft/Patient Misidentification Policy 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 hospital 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 Health Information Management/Medical Records office, 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,

_____

Privacy/Compliance Officer

St. Joseph's Healthcare System

973-754-3565

Exhibit E to Identity Theft/Patient Misidentification Policy

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 St. Joseph's {Medical Center / Wayne Hospital} ("SJHS") 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 of another person who 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 (DATE) _____because {we have determined/you have indicated}you did not receive services at this hospital on those dates. After removing that information, your medical record shows the following visit.

Date of Visit Reason for Visit

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 the facility's Health Information Management office by scheduling an appointment with the Director by calling 973-754-2995/6 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 SJHS can assist you, or should you have any questions, please do not hesitate to contact me.

Sincerely,

_____

Privacy/Compliance Officer

973-754-3565

Exhibit F to Identity Theft/Patient Misidentification Policy

Checklists of Action Items **(**check all that apply)

When Identity Theft Is Alleged

1. Advise victim to report identity theft incident to law enforcement and indicate that paperwork will be forwarded for victim to complete.

2. Complete and send victim report of ID theft letter (Exhibit A), with a copy of the FTC Identity Theft affidavit (Exhibit B) to be completed by victim.

3. When victim's allegation is supported by a properly completed and signed FTC Identify Theft Affidavit, flag the victim's account so that medical personnel know the medical record may contain inaccurate information.

4. Follow appropriate steps below for Identity Theft or Misidentification.

When Identity Theft is Reasonably Suspected or Known to have Occurred

1. Complete Exhibit C (Identity Alert reporting form).

2. Route copies of Exhibit C with a copy of the relevant photo ID to SJHS's □

Privacy/Compliance Officer, HIM Director, Security Director, Registration Director,

Patient Accounts Director and Legal Affairs.

3. The Patient Accounts Director will put affected patient accounts on hold pending □ the outcome of the investigation.

4. The Privacy/Compliance Officer will review and make a recommendation on the □ investigation and external reporting and notification decisions.

E.g., victim notification; fraud to the Medicaid OIG at 1-800-866-633-6585 incidents involving mail theft, will direct reporting to U.S. Postal Inspection

Service; if identity theft involves unauthorized access of unencrypted *computerized* data, special reporting will occur in accordance with New Jersey law; and coordinating with area health care providers.

5. If identity theft or theft of services has occurred and the value of the services in □ question report the exceeds $500, the Privacy/Compliance Officer, after discussion with General Counsel, will instruct the Security Department to report the incident to the appropriate law enforcement agency, subject to the information limitations in Section 4(C). The Security Department will obtain the investigating officer's name and phone number, and will consult with law enforcement about the timing and the content of any victim notification.

6. The Privacy/Compliance Officer will notify victims of identity theft as directed by the after consultation with law enforcement. Use the letter regarding identity theft (Exhibit D) to notify a victim of identity theft and include the FTC Identity Theft Affidavit (Exhibit B).

7. The HIM Department will correct the medical record in accordance with Section

4(E)(i) and document and forward to the Compliance office the patient's verification of the corrected medical record shall be documented and included as part of the case file forwarded to the Compliance office.

8. The Billing Department will correct the patient's billing information and make all necessary payment adjustments in accordance with Section 4(E)(ii).

The patient's verification of the corrected billing record shall be documented and included as part of the case file forwarded to the Compliance office.

9. The Privacy/Compliance Officer will determine whether accounting for disclosures to the identity theft suspect is required.

10. The Registration Director will add an MPI Alert Flag of "Identity issue/ call Security" to each MPI record affected by the identity theft event.

11. Once the Registration Director and/or the Patient Accounts Director verify that all demographic and insurance information is correct after the visit is transferred to the appropriate MPI record and all related documents are removed from the permanent record and replaced with appropriately revised documents, the bill hold will be released so that appropriate billing occurs.

12. Identity theft suspect will be billed for services and litigation will be considered.

13. Either the Registration Director or Privacy/Compliance Officer will update the SJHS Identity Theft Database with the Identity Alert Form.

14. A copy of all documentation concerning identity theft will be provided to the Compliance office to be maintained.

OCCURRENCE OF PATIENT MISIDENTIFICATION

Patient Misidentification—Investigation and Notification

1. Complete Exhibit C (Identity Alert reporting form).

2. Route copies of Exhibit C with a copy of the relevant photo ID to the Privacy/Compliance Officer, HIM Director, Security Director, Registration Director, Patient Accounts Director, and General Counsel.

3. The Patient Accounts Director will put affected patient accounts on hold pending the outcome of the investigation.

4. The Privacy/Compliance Office will review and a recommendation on the investigation and make all external reporting and notification decisions. E.g., patient notification; notification of patient in the event of unauthorized access of unencrypted *computerized* data resulting in security breach.

5. The HIM Department will notify patients affected by patient misidentification using Exhibit E.

6. The HIM Department will correct the medical record in accordance with Section

5(D)(i) and document and forward the patient's verification of the corrected medical record to the Compliance office and included as part of the case file forwarded to the Compliance office.

7. The Billing Department will correct the patient's billing information and make all necessary payment adjustments in accordance with Section 5(D)(ii). The patient's verification of the corrected billing record shall be documented and included as part of the case file forwarded to the Compliance office.

8. Once the Registration Director and/or the Patient Accounts Director verify that all demographic and insurance information is correct after the visit is transferred to the appropriate MPI record and all related documents are removed from the permanent record and replaced with appropriately revised documents, the bill hold will be released so that appropriate billing occurs.

9. The Privacy/Compliance Officer will determine whether accounting for disclosures is required.

10. A copy of all documentation concerning patient misidentification must be provided to the Compliance office.