		SUBJECT: Identity Theft / Patient Misidentification **POLICY NUMBER:** **Page 1 of 16**	
		GENERATED BY: Integrity Compliance Office	
		APPROVED BY:	
ISSUED: 11/7/06	**REVISED: 3/16/07; 5/6/08 (web reference updates only)**	**REVIEWED:**	**REFERENCE:**

Scope

All XXXXX XXXXX operations

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 hospital or other facility accesses the wrong medical record so that the medical records of two patients are commingled.

Policy

XXXXX XXXXX entities 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. Hospital 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 nonphoto 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 XXXXX XXXXX Master Patient Index call the Registration Supervisor or the applicable Privacy 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 and registration staff may offer to take a photograph of the patient in accordance with any approved registration staff photograph policy. Refer to Photo Identification of Patients Policy.

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 XXXXX XXXXX's master-patient index 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 facility Privacy Officer. The Registration Supervisor/Privacy 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.).

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. Complete and send the letter attached as Exhibit A with a copy of the 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 the 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 the identity theft allegation is supported by an FTC Identify Theft Affidavit, the facility must flag the account of the patient alleging identity theft so that 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 without consent or lawful authority, the facility shall take the following steps:

A. Notifications. When identity theft is reasonably suspected or is known to have occurred by an employee (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 of the same to the entity Privacy Officer, HIM Director, Security Director, Registration Director, Patient Account Director, and the XXXXX XXXXX Integrity-Compliance office. Attach a copy of the relevant photo ID. If the incident occurs on a weekend, reporting should occur the next business day. The Integrity-Compliance Office will review and make decisions on the finding and make all external reporting and notification decisions. External notification and reporting will occur only as directed by the Integrity-Compliance Office.

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 must be reported immediately to the Medicaid OIG: 1-800-###-####.

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 code, access code, or password that would permit access to an individual's

financial account, the Integrity Compliance Office will direct reporting in accordance with <State> Code Ann.§ <Section> to any resident of <State> whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. 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-XXXXX XXXXX health care providers about the possibility of identity theft in connection with the victim's identifying information. *See* XXXXX XXXXX HIPAA Policy, *"Authorization to Release Information*." However, in the event circumstances indicate that the identity thief may imminently use the victim's information to defraud a non-XXXXX XXXXX 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-XXXXX XXXXX provider to prevent further fraudulent activity in connection with the victim's identifying information, the Integrity-Compliance office may disclose (or direct disclosure) to a non-XXXXX XXXXX provider information about the identity theft victim 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-XXXXX XXXXX 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-XXXXX XXXXX provider, the victim's written authorization must be obtained prior to releasing any identifying information about the victim to a non-XXXXX XXXXX 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 entity 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 Integrity-Compliance office. If the Integrity-Compliance office together with the entity believe in good faith that identity theft or theft of services has occurred on the entity's premises, and the value of the services in question exceeds or may exceed $500, the Integrity-Compliance office will instruct the entity's Security Department to report the incident to the law enforcement agency in the city or county in which the facility is located. In order to facilitate reporting and efficient prosecution of identity theft crimes, the entity should prepare a summary of the information that the entity believes in good faith constitutes evidence of criminal conduct that occurred on the entity'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.

i. Substance Abuse Treatment Facilities. Reporting by a federally-funded substance abuse program should be limited to the circumstances of the incident, including the patient status of the individual committing or threatening to commit identity theft, that individual's name

and address, and that individual's last known whereabouts. No other information may be provided.

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 HIM department as directed by the Integrity-Compliance office. The letter attached to this Policy as Exhibit D may be used as a form 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 entity's 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 entity's medical record corrections policy and XXXXX XXXXX HIPAA Policy, *Amendment of Health Information*. A detailed explanation of the corrections shall be generated by the entity and verified by the patient. Pursuant to XXXXX XXXXX HIPAA Policy, 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 Optical System and make replacements with appropriately revised documents. The patient's verification of the corrected medical record shall be documented and included as part of the case file forwarded to the Integrity-Compliance office.

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 entity's 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 the entity's billing record corrections policy and XXXXX XXXXX HIPAA Policy, *Amendment of Health Information*. A detailed explanation of the corrections shall be generated by the entity 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 Integrity-Compliance office.

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

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 the Optical System 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 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 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 which 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 facility may refuse to provide business transaction records if the facility determines 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 known to the entity, the facility may bill the identity theft suspect for unlawfully obtained services. If a suspect is identified and the entity has suffered an ascertainable loss (such as by providing services never paid for), the entity may consider pursuing a civil claim. Consult with the Integrity-Compliance office for further guidance.

H. Accounting for Disclosures. The entity's Privacy Officer should determine whether, as result of identity theft, protected health information was inappropriately disclosed. If protected health information was inappropriately disclosed, the entity's HIM department must account for such disclosures in accordance with the XXXXX XXXXX HIPAA Policy, *Accounting for Disclosures*.

I. Update Identity Theft Database. When identity theft is reasonably suspected, either the Registration Director or the facility's Privacy Officer must update the XXXXX XXXXX 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 attached as Exhibit C and route copies of the same to the entity Privacy Officer, HIM Director, Security Director, Registration Director, Patient Account Director, and the XXXXX XXXXX Integrity-Compliance office. Attach a copy of the relevant photo ID. If the incident occurs on a weekend, reporting should occur the next business day. The Integrity-Compliance Office will review and make decisions on the finding and make all external reporting and notification decisions. External notification and reporting will occur only as directed by the Integrity-Compliance Office. For example, the Integrity-Compliance office will direct the following reporting:

i. Security Breach If the event 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 Integrity Compliance Office will direct reporting in accordance with <State> Code Ann.§ <Section> to any resident of <State> whose unencrypted personal information was or is reasonably

believed to have been acquired by an unauthorized person. 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. Patients affected by patient misidentification will be notified by the HIM Department as directed by the Integrity-Compliance office. The letter attached to this Policy as Exhibit E may be used as a form 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 entity's 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 entity's medical record corrections policy and XXXXX XXXXX HIPAA Policy, *Amendment of Health Information*. A detailed explanation of the corrections shall be generated by the entity and verified by the patient. Pursuant to XXXXX XXXXX HIPAA Policy, 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 Optical System and make replacements with appropriately revised documents. The patient's verification of the corrected medical record shall be documented and included as part of the case file forwarded to the Integrity-Compliance office.

ii. Payment Records. After appropriate consultation with and input from the patient (whose identity has been properly verified and documented), the entity's 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 the entity's billing record corrections policy and XXXXX XXXXX HIPAA Policy, *Amendment of Health Information*. A detailed explanation of the corrections shall be generated by the entity 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 Integrity-Compliance office.

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 the Optical System 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.

E. Accounting for Disclosures. The entity's Privacy Officer should determine whether, as result of patient misidentification, protected health information was inappropriately disclosed. If protected health information was inappropriately disclosed, the entity's HIM department must account for such disclosures in accordance with the XXXXX XXXXX HIPAA Policy, *Accounting for Disclosures*.

6. Documentation. A copy of all documentation concerning identity theft or patient misidentification must be provided to the Integrity-Compliance office.

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.

References: <State>C.A. § <Section> (identity theft crime); <State>C.A. § <Section> (theft of services crime); 45 C.F.R. § 164.512(f)(5) (HIPAA crime on premises); 42 C.F.R. § 2.12 (c)(5)(ii);<State>C.A. § <Section> (reporting requirement for unauthorized access to certain computerized data). <State>C.A. § <Section> et seq. (TCPA – civil claims against identity thieves); <State>C.A. § <Section> et seq. (<State> Identity Theft Deterrence Act of 1999 – civil claims against thieves).

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 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 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,

_____
_____

Enclosure (FTC Identity Theft Affidavit)

Exhibit B to Identity Theft/Patient Misidentification Policy
FTC ID Theft Affidavit

Exhibit C to Identity Theft/Patient Misidentification Policy

IDENTITY ALERT FORM

This form should be completed by 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:_____
_____
_____
Approximate Cost of Visit: _____
Existing MPI Used:_____ New MPI 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 (such that the 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 FACILITY'S PRIVACY OFFICER; REGISTRATION DIRECTOR; SECURITY DIRECTOR; PATIENT ACCOUNT DIRECTOR; AND THE XXXXX XXXXX INTEGRITY-COMPLIANCE OFFICE

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 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 Officer
[Facility]
[Telephone number]

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 [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 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 _____ 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 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 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]

Exhibit F to Identity Theft/Patient Misidentification Policy
Checklists of Action Items

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 remainder of the steps.

When Identity Theft is Reasonably Suspected or Known to have Occurred

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

6. Route copies of Exhibit C with a copy of the relevant photo ID to the entity's Privacy Officer, HIM Director, Security Director, Registration Director, Patient Accounts Director, and the XXXXX XXXXX Integrity-Compliance office.

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

8. The Integrity-Compliance Office will review and make decisions on the investigation and make all external reporting and notification decisions. E.g., victim notification; the Integrity-Compliance Office will direct reporting of actual knowledge of Medicaid fraud to the Medicaid OIG at 1-800-###-####; for 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 <State> law; and coordinating with area health care providers.

9. If identity theft or theft of services has occurred and the value of the services in question report the exceeds $500, the Integrity-Compliance Office will instruct the Security Department to 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.

10. The HIM Department will notify victims of identity theft as directed by Integrity- Compliance Department 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).

11. The HIM Department will correct the medical record in accordance with Section 4(E)(i) and document and forward to the Integrity-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 Integrity-Compliance office.

12. 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 Integrity-Compliance office.

13. The entity's Privacy Officer will determine whether accounting for disclosures to the identity theft suspect is required.

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

15. 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 Optical System/replaced with appropriately revised documents, the bill hold will be released so that appropriate billing occurs.

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

17. Either the Registration Director or the facility's Privacy Officer will update the XXXXX XXXXX Identity Theft Database with the Identity Alert Form.

18. A copy of all documentation concerning identity theft will be provided to the Integrity-Compliance office.

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 entity's Privacy Officer, HIM Director, Security Director, Registration Director, Patient Accounts Director, and the XXXXX XXXXX Integrity-Compliance office.

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

4. The Integrity-Compliance Office will review and make decisions 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, as directed by the Integrity-Compliance Office, 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 to the Integrity-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 Integrity-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 Integrity-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 Optical System/replaced with appropriately revised documents, the bill hold will be released so that appropriate billing occurs.

9. The entity's Privacy Officer will determine whether accounting for disclosures is required.

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