ORGANIZATION POLICY

POLICY TITLE: IDENTITY THEFT PREVENTION

POLICY NUMBER: 1227

I. POLICY

It is the policy of Onslow Memorial Hospital ("OMH") to follow laws and reporting requirements regarding fraud and abuse in healthcare. Federal laws prohibit the willful or knowing misrepresentation of personal identity for fraudulent purposes, including the deliberate use of an inappropriately obtained social security number (SSN), ID card, etc. to obtain healthcare. North Carolina law also prohibits the willful or fraudulent possession or use of false identification information. The Compliance Committee in connection with Risk Management is responsible for: (i) implementing and maintaining a written Identity Theft Prevention Program to detect, investigate, and mitigate potential identity theft/fraud and abuse ("the Program") without negatively impacting appropriate care of patients or compliance with the Emergency Medical Treatment and Active Labor Act (EMTALA); and (ii) training appropriate staff accordingly.

II. PURPOSE

This policy establishes procedures for staff members to follow to ensure the protection of patients' medical and financial records in compliance with various federal and state identity theft laws, including the Red Flags Rule under the Fair and Accurate Credit Transactions Act.

III. DEFINITIONS

A. **Identifying Information.** The following are considered identifying information for purposes of this policy:

i. Social security or employer taxpayer identification numbers;

ii. Drivers license, State identification card, or passport numbers (except drivers' license numbers appearing on law enforcement records);

iii. Checking and savings account numbers;

iv. Credit and debit card numbers;

v. Personal Identification ("PIN") codes;

vi. Any other numbers or information that could be used to access a person's financial resources;

vii. Biometric data;

viii. Fingerprints; and

ix. Passwords.

B. **Identify Theft.** When a person knowingly transfers or uses without legal authority a means of identification of another person with the intent to commit, or to aid and abet, any unlawful activity that constitutes a violation of Federal law or that constitutes a felony under any applicable North Carolina or local law.

C. **Medical Identity Theft.** When an individual assumes or attempts to assume the identity of another person through fraudulent means or false pretenses and obtains or attempts to obtain medical service or goods, or to make false claims for medical services or goods. Medical identity theft can be devastating to the individual whose information was fraudulently used. It also presents financial, operational, and administrative difficulties for health care providers.

D. **Personal Information.** A person's first name or first initial and last name in combination with identifying information.

E. **Red Flags.** Patterns, practices and specific activities signaling possible identity theft in connection with OMH, and which include, but are not limited to the following circumstances:

i. Patient presents for an episode of care and is recognized as someone other than the patient presenting him/herself to be;

ii. Patient submits a driver's license, insurance card or other identifying information that appears to have been altered or forged;

iii. Photograph on a driver's license or other photo ID card submitted by the patient does not resemble the patient;

iv. Information on one form of identification submitted by the patient is inconsistent with information on another form of identification, or with information already in the Hospital's records;

v. Discrepancies between admissions information and prior account information or current insurance eligibility information;

vi. The physical address provided by the patient is known not to exist, or the patient cannot provide anything other than a post office box as physical address;

vii. Address or name discrepancy on identification or insurance information;

viii. The Social Security Number (SSN) furnished by the patient has not yet been issued, is listed on the Social Security Administration's Death Master File, or is otherwise invalid. The following numbers are known to be invalid:

(a) The first three digits are in the 800, 900 or 000 range, are in the 700 range above 772, or are 666;

(b) The forth and fifth digits are 00; and

(c) The last four digits are 0000.

ix. Unusual use or suspicious activity related to a patient account, or notice from customers, law enforcement or others of unusual activity related to that account;

x. Dispute by a patient concerning the validity of a bill or OMH services, including a complaint or question related to a patient's receipt of a bill for another individual; a bill or explanation of benefits (EOB) for a OMH product or service the patient claims he or she did not receive; or a bill from a OMH

provider from whom the patient did not receive care; and

xi. Receipt of any notice or inquiry into potential identity theft, including those received from an investigator, private insurance company, or law enforcement agency.

F. **Security Breach.** An incident of unauthorized access to and acquisition of unencrypted and un-redacted records or data containing identifying information where illegal use of the information has occurred or is reasonably likely to occur or that creates a material risk of harm to an individual. Any incident of unauthorized access to and acquisition of encrypted records or data containing identifying information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of OMH for a legitimate purpose is not considered a security breach, provided that the information is not used for a purpose other than a lawful purpose and is not subject to unauthorized disclosure.

IV. PROCEDURES

OMH will take all reasonable steps to prevent, detect, respond to and mitigate known or suspected security breaches with respect to personal and identifying information as defined above.

A. Detecting Red Flags

i. In order to detect potential identity theft, OMH will request the following information and documents at time of registration.

(a) Driver's license, passport, state identification card, or other photo identification (such as employment ID); **and**

(b) Any two (2) of the following:

1. Social Security Number and Social Security card (if available);
2. Date of birth;
3. Physical address and telephone number;
4. Insurance card (if available); and
5. Other verification of identity, such as voter's registration card or credit card.

ii. If the patient does not provide the requested information and documentation, the registrar will consult his/her supervisor to determine appropriate action, *with the following exceptions:*

(a) Emergency Department: OMH will provide a medical screening examination for any individual presenting to the Emergency Department, regardless of whether the information listed above is provided.

(b) Prior Verification: If the OMH entity has provided services to the patient within the preceding six (6) months and the patient's name, date of birth, SSN, address and signature match the prior record, documentation of identity is not required.

B. Breaches and Notifications

i. Responding to Complaints of Identity Theft

Medical Identity Theft: If a patient notifies OMH of possible identity theft in regard to their medical record or bill, the investigation will be coordinated with the appropriate department(s) (e.g., Patient Financial Services and Medical Records) pursuant to OMH established departmental procedures. Risk Management will make any necessary reports to external agencies.

Suspected Medical Identity Theft in the Emergency Department: If a person presents to the OMH Emergency Department for emergency treatment and identify theft/fraud is suspected, a medical screening examination will be performed and any identified emergency medical condition will be stabilized as appropriate prior to initiating investigational activity. Risk Management should be contacted as soon as practical for further investigation and verification of the person's identity.

ii. Internal Notifications

Any OMH employee who becomes aware of a potential or actual breach of personal information or medical history must make immediate report to Risk Management who will then notify the OMH Privacy and Compliance Officers. Investigations will be conducted pursuant to established Risk Management policies/procedures.

(a) If unable to verify the patient's information, Risk Management (or designee) shall, after obtaining the appropriate physician approval, politely decline treatment until OMH is able to verify the patient's identification and offer to reschedule for a future date after identification information verification is completed.

(b) If, after speaking with the patient, the patient presents different information, Risk Management will proceed to gather the new information and process verification as noted above.

iii. External Notification

Risk Management will work with OMH Legal Counsel and the appropriate OMH departments to determine if any reports to outside agencies are required.

iv. Required Notification to the Affected Individual

OMH may be required to notify affected individuals of potential or actual security breaches. Each potential notification of breach will be reviewed by

OMH Legal Counsel and other appropriate departments (e.g., Privacy, IT Security, and Compliance). If it is determined that a reportable security breach has occurred, OMH shall take appropriate action including the following:

(a) Notifying the affected individuals without unreasonable delay, with all of the following information:

1. Description of the incident in general terms;

2. The type of identifying information that was subject to the unauthorized access and acquisition;

3. The general acts of the OMH to protect the personal information from further unauthorized access;

4. The person and telephone number that the person may call for further information and assistance; and

5. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Notice to the affected persons will be considered proper if provided by one or more of the following methods:

1. Written notice

2. Telephone notice, provided contact is made directly with the affected person(s) and appropriately documented.

3. Substitute notice may include emailing the affected person(s) if the entity has their email addresses, and/or notifying local or statewide media sources. Substitute notice may be given if:

   (i) The cost of providing the notice exceeds $250,000;

   (ii) The number of affected persons is greater than $500,000, or

   (iii) The entity does not have the necessary contact information to notify the individual in any of the methods noted above.

(b) Providing the affected individual(s) with information about how to alert credit agencies to potential fraud and identity theft.

v. Optional credit monitoring services

If appropriate, OMH may offer the individual(s) affected the option of enrolling in a credit monitoring service for a defined period of time. The determination of whether and for how long to offer this service will depend on the nature and extent of the potential or actual breach, and will be made by the appropriate department in consultation with OMH Legal Counsel.

vi. Delayed Notice

Notice shall be delayed if law enforcement informs OMH that disclosure of the breach would impede a criminal investigation or jeopardize national security. A request for delayed notification must be made in writing or documented contemporaneously by the entity in writing, including the name of the law enforcement officer making the request and the officer's agency engaged in the investigation. The required notice shall be provided without unreasonably delay after the law enforcement agency communicates to the entity its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

vii. Additional Notice Requirements

If a security breach involves more than 1,000 persons, OMH will provide written notice of the timing, distribution, and content of the notice to the Consumer Protection Division of the North Carolina Attorney General's Office, as well as to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p). In addition, OMH will submit to the Consumer Protection Division a completed "North Carolina Security Breach Reporting Form" which includes the number of North Carolina residents affected and the total number of persons affected. (Attached as Exhibit "A")

C. Institutional Actions

At least annually, OMH Privacy and Security Officer(s) will review all incidents of actual or potential security breaches and make recommendations to OMH Senior Management for institutional improvements in order to minimize such occurrences in the future and to identity any changes in risk.

EFFECTIVE DATE: April 30, 2009

APPROVED BY:

Ed Piper, Ph.D.
President and Chief Executive Officer

Penney Burlingame, RN, MHA, FACHE
Senior VP Nursing and Clinical Services

Crystal Hayden, RN, MSN
Senior VP Chief Nursing Officer

Michael Josilevich, M.D.
Chief of Staff