San Antonio Metropolitan Health District	Immunization Program	Policy Number 2 Page 1 of 7
Approved By: Vivian Flores, Immunization Program Manager		Effective Date: June 15, 2012
Subject: San Antonio Immunization Registry System (SAIRS) Security and Confidentiality Policy		Review Date: January 1, 2014

I. **PURPOSE**: This document shall govern the administrative, physical, and technical safeguards necessary to protect the confidentiality, availability, and integrity of information in the San Antonio Immunization Registry System, herein referred to as "SAIRS" or "Registry". Implementation of these safeguards is intended to reduce risks and minimize effects associated with unauthorized disclosure, access, alteration, deletion, and transmission of data collected and maintained in the Registry.

II. **BACKGROUND**: SAIRS is a Web-based immunization information system that is capable of establishing and maintaining a repository of lifespan immunization data for the population of the City of San Antonio, Bexar County, Texas, and surrounding areas. The purpose of SAIRS is to consolidate immunization information among health-care providers, ensure adequate immunization levels, and avoid duplicate or unnecessary immunizations. SAIRS was developed through the efforts of Metro Health and the Centers for Disease Control and Prevention.

Individual participation in the Registry is voluntary. Immunization records may be included in SAIRS unless the individual or parent/guardian has submitted a *Request to Opt Out of SAIRS* form.

III. **DEFINITIONS**:

Authorized Users: Those individuals and/or entities that require regular access to patient immunization records and other protected health information (PHI) to: (1) provide immunization services to patients, (2) maintain a computerized inventory of their public and private stock of vaccine, (3) assess immunization status, (4) ensure compliance with school and child-care immunization requirements, or (5) collect data about the quality of care and services provided by health plans. Metro Health's Immunization Program Manager determines if these potential users have a legitimate need for access.

CoSA: City of San Antonio.

Health Sensitive Information Area: The area is a separate location at ITSD's data center. The area physically isolates servers from other data center operations and is isolated from the CoSA network.

HEDIS: HEDIS (Healthcare Effectiveness Data and Information Set) is a tool used by health plans to measure performance on important dimensions of care and service, including childhood and adolescent immunization status.

HTTPS: Hypertext Transfer Protocol over Secure Sockets Layer (SSL). HTTPS is used by Web servers to transfer and display Web content securely. The data transferred using HTTPS is encrypted so that it cannot be read by anyone except the recipient.

HIPAA: Health Insurance Portability and Accountability Act of 1996.

ITSD: CoSA's Information Technology Services Department.

ImmTrac: The statewide immunization registry managed and operated by the Texas Department of State Health Services.

Metro Health: San Antonio Metropolitan Health District.

PHI: Protected Health Information, or "individually identifiable health information." The U.S. Department

of Health and Human Services defines this information as "information, including demographic data, that relates to: (1) the individual's past, present or future physical or mental health or condition; (2) the provision of health care to the individual; or (3) the past, present, or future payment for the provision of health care to the individual; and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, date of birth, and Social Security Number)."

SAIRS: San Antonio Immunization Registry System.

SSL (Secure Sockets Layers) **Certificate**: A digital certificate used for securing data transferred over the Internet.

IV. POLICY STATEMENT

It is the policy of the Metro Health Immunization Program to comply with the requirements of Texas Health and Safety Code, Chapter 181, Subchapter D, and federal HIPAA Standards for Privacy of Individually Identifiable Health Information (45 CFR, Part 160, and Subparts A and E of Part 164). Metro Health shall take reasonable measures to protect the health information contained within SAIRS from physical, technical, and administrative loss, theft, and unauthorized use and access.

V. USES OF REGISTRY INFORMATION

Registry information shall be entered by and available to authorized users for the uses defined herein.

1. SAIRS immunization data and other PHI shall be used by authorized users for the purposes of:

a) Creating, consolidating, maintaining, and accessing computerized immunization records;

b) Tracking and maintaining vaccine inventory information;

c) Determining the immunization history of a patient and delivering health-care treatment accordingly;

d) Generating reminder notices for patients who are due or overdue for immunizations;

e) Generating informational notices to patients who have received a vaccine that has been recalled;

f) Assessing the immunization rates of a clinic's patient population;

g) Generating official immunization records;

h) Ensuring compliance with mandatory immunization requirements for schools and child-care centers;

i) Recording the distribution and use of countermeasures in response to a public health emergency;

j) Fulfilling other purposes determined at the discretion of Metro Health's Immunization Program Manager.

2. SAIRS immunization data and other PHI shall be utilized by Metro Health's Immunization Program for the purposes of:

a) Performing quality improvement and quality assurance activities;

b) Assessing compliance with the Vaccine for Children Program requirements;

c) Preventing and responding to outbreaks of vaccine-preventable diseases;

d) Reporting on activities relating to grant performance;

e) Producing reports to aid in the development of policies and strategies to improve public health;

f) Populating ImmTrac once a patient or patient's parent/guardian has consented to ImmTrac participation, in accordance with ImmTrac consent rules;

g) Managing and maintaining the Registry system; and

h) Fulfilling other purposes determined at the discretion of Metro Health's Immunization Program Manager.

3. Metro Health's Immunization Program may provide member information from SAIRS to health plans for billing and HEDIS reporting purposes.

VI. ROLES AND RESPONSIBILITIES

1. Metro Health is a public health agency authorized to receive information without patient authorization for the purposes of preventing and controlling disease. Metro Health's Immunization Program shall:

a) Provide the resources and guidance necessary to support the privacy, confidentiality, and security of information contained in SAIRS.

b) Ensure the confidentiality and security of SAIRS information by instituting procedures that encompass the administrative, physical, and technical safeguards of the Registry (e.g., *SAIRS Facility Enrollment Form* and *SAIRS User Confidentiality and Security Agreement*).

c) Provide registry security awareness training as well as training on the use of SAIRS to authorized users.

d) Designate a Registry Program Coordinator responsible for assessing and taking corrective action of potential risks and vulnerabilities to the information confidentiality, data integrity, and system availability of SAIRS.

e) Designate a SAIRS Application Administrator(s) responsible for user access control administration, in accordance with this policy and data quality assurance. The SAIRS Application Administrator(s) shall:

(1) Create and maintain user accounts.

(2) Implement procedures to ensure that only legitimate users are granted access to SAIRS.

(3) Ensure that access to SAIRS is granted only after a user has signed the SAIRS User Security and Confidentiality Agreement.

(4) Monitor SAIRS user activity and application logs for inappropriate activity.

(5) Apply the principle of least privilege when assigning SAIRS user accounts.

(6) Grant individual user access based upon the individual's job duties.

(7) Monitor the accuracy and quality of data within SAIRS and take corrective action if necessary.

(8) Periodically review safeguards and provide policy guidance regarding SAIRS.

(9) Remove all immunization data on a patient record from the Registry when a patient, parent, or guardian submits a *Request to Opt Out of SAIRS* form.

2. ITSD shall:

a) Physically secure all SAIRS server equipment in the Health Sensitive Information Area.

b) Implement and maintain a backup and recovery schedule that will ensure a 24-hour recovery time objective (RTO) and a four-hour recovery point objective (RPO).

c) Maintain safeguards to protect against a defined threat to SAIRS, its resources, and its data.

d) Maintain audit logs within the SAIRS database for at least 6 years.

e) Secure data while in transport through the use of SSL certificate and HTTPS or other encryption technologies.

3. All authorized users shall:

a) Protect registry information from unauthorized access and misuse of information;

b) Protect each username and password from discovery and never share passwords with anyone.

c) Access SAIRS only for legitimate immunization purposes relating to the user's job duties; legitimate uses are described in Section V: Uses of Registry Information.

d) Limit unauthorized physical access to computer systems, displays, networks, and immunization records.

e) Ensure that printouts of SAIRS immunization records and reports are secure

from unauthorized access.

4. Facility enrollees (e.g., physicians, nurses, clinic staff, and Metro Health staff) shall:

a) On behalf of the Metro Health Immunization Program, notify patients, parents, or guardians of their right to have their information excluded from SAIRS. Enrollees shall display or provide the attached Disclosure Statement to patients, parents, or guardians.

b) Provide a *Request to Opt Out of SAIRS* form to the patient, parent, or guardian when the patient, parent, or guardian elects to withhold or withdraw information from SAIRS.

c) Seek patient or parental consent for ImmTrac participation and record consent in SAIRS. The signed ImmTrac consent shall be stored in the patient's file. Metro Health may provide immunization records to ImmTrac, when patient or parental consent has been indicated in SAIRS.

d) Promptly notify the SAIRS Application Administrator when authorized users discontinue employment or require a change in access rights.

e) Promptly notify the Registry Coordinator or SAIRS System Administrator of any threat to the security and confidentiality of SAIRS information.

f) Implement reasonable administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of the information contained in SAIRS.

5. Patients, parents, and guardians shall:

a) Submit a completed and signed *Request to Opt-Out of SAIRS* form, when electing to opt out of the registry, to

Metro Health – Immunization Program
SAIRS Opt Out
332 W. Commerce, Suite 108
San Antonio, TX 78205

Note: The registry will retain only core demographic information necessary to identify the patient who has chosen to opt out of SAIRS. This information is necessary to enable the Registry to filter and refuse entry of immunization information for the patient. Additionally, any prior immunization records associated with the client will be deleted from the Registry.

b) Submit a completed and signed *Request to Opt Into SAIRS* form, when a *Request to Opt Out of SAIRS* form has been processed and the patient, parent, or guardian wishes to once again participate in the Registry.

VII. SAFEGUARDS

1. The following administrative safeguards shall be implemented to ensure the confidentiality, integrity, and security of the information contained in SAIRS.

a) Each year, in conjunction with the update of the SAIRS Business Plan, the

Registry Coordinator shall conduct a risk analysis that identifies potential security risks. Risks identified shall be addressed in the SAIRS Business Plan.

b) The Registry Program Coordinator and/or the SAIRS Application Administrator shall regularly review records of SAIRS activity, such as audit logs, access reports, and security incident reports.

c) In accordance with Metro Health's *Notice of Privacy Practices*, patients may inspect and obtain a copy of their or their child's immunization record. Corrections or amendments to a record shall be made by an authorized user only when the patient or parent/guardian is able to demonstrate, through a credible source, that the record is incorrect. Credible sources include, but are not limited to, immunization records provided by: state, local, or national immunization registries; the patient's doctor; or a hospital.

d) User access to SAIRS shall be granted only after the user's affiliated organization has completed and submitted a signed *SAIRS Facility Enrollment Form* to the Metro Health Immunization Program and the user has submitted a signed *SAIRS User Security and Confidentiality Agreement.*

e) Authorized SAIRS users may provide an official immunization record to persons who have shown proof of identity and are:

(1) the patient, if over 18 years old or emancipated;

(2) the minor patient's parent or guardian;

(3) the minor patient's grandparents, brother, sister, aunt, or uncle when presenting the patient for vaccine administration (the presenting relative must be at least 18 years of age); or

(4) any person who can produce a written authorization from the patient, parent, or guardian. The authorization must include the patient's name, date of birth, current address, a telephone number to confirm authorization, and the patient's health-care provider's name.

Note: SAIRS users shall not provide any PHI to persons whom the patient, parent, or guardian has specifically identified as not authorized to receive such information. Providers should notate these restrictions as a patient note.

2. The following physical safeguards shall be implemented to ensure the confidentiality, integrity, and security of the information contained in SAIRS.

a) Users shall ensure that their computer screen is not easily viewable by persons not authorized to view a particular patient record.

b) Reasonable steps shall be taken to ensure that the SAIRS server environment is protected from unauthorized physical access, tampering, theft, and physical damage, while ensuring that access by properly authorized Metro Health or ITSD employees is granted.

3. The following technical safeguards shall be implemented to ensure the confidentiality, integrity, and security of the information contained in SAIRS:

a) Users shall be automatically logged off of the Registry after 30 minutes of inactivity.

b) Unique identifiers and passwords are used to authenticate users and make it possible to hold users accountable for their actions.

c) SAIRS user accounts shall be automatically locked after three failed password attempts;

d) SAIRS shall enforce a strong password policy. Passwords shall:

(1) be a minimum of eight characters;

(2) contain both upper and lower cases letters;

(3) contain at least one number;

(4) contain at least one symbol;

(5) expire every 120 days; and

(6) not be reused for a minimum of occurrences as defined by the SAIRS Administrator.

e) Application logs shall record all transactions of access to patient information.

f) All PHI is encrypted before transmission over the Internet. The SAIRS application is secured through the use of an SSL certificate.

VIII. ATTACHMENTS (OPTIONAL): *SAIRS Facility Enrollment Form, SAIRS User Security and Confidentiality Agreement, SAIRS Notice to Patients and Parents, Request to Opt Into SAIRS, Request to Opt Out of SAIRS*

Approved by:

Vivian Flores
Metro Health Immunization Program Manager

6/11/12
Date