ImmTrac
Texas Immunization Registry

Quality Assurance Processes

Version 1.04
April 5, 2005

For comments or questions about this document, please contact:

Claude Longoria, Manager
ImmTrac Group
Texas Department of State Health Services
1100 W. 49th St.
Austin, TX 78756
(512) 458-7111 ext. 6454
Claude.Longoria@dshs.state.tx.us

TEXAS
Department of
State Health Services

TABLE OF CONTENTS

1. Program Overview

ImmTrac, the Texas immunization registry is a confidential central repository of immunization records for Texas children under 18 years of age designed to consolidate immunization records from multiple sources statewide to provide the most complete immunization history for a child. ImmTrac contains over 41 million immunization records for more than 5 million Texas children. The use of immunization registries has been shown to improve vaccine coverage levels. ImmTrac is a major component of the Texas Department of State Health Services (DSHS) strategy to increase immunization rates in Texas. (Appendix A)

The ImmTrac system continually receives new client and immunization information either through the GUI (Graphical User Interface) or through the import process, which reads flat files containing client and immunization updates. Although ImmTrac's on-line Web interface is the most visible method for adding and updating children's demographic and immunization data, imported data is expected to continue as the largest source of records for the registry.

The registry's usefulness is based on the quality and integrity of the immunization data it contains. This document presents an overview of the Quality Assurance processes and procedures employed by DSHS immunization registry staff, DSHS IT staff, and contractor staff (Electronic Data Systems, EDS) follow when processing data received from providers and payors to ensure quality in the collection and reporting of data, to protect and ensure the quality of ImmTrac data, and to maintain the utility of the ImmTrac system.

2. Legislation and Rules

Texas Health and Safety Code, Section 161.007 mandates that DSHS, "for purposes of establishing and maintaining a single repository of accurate, complete, and current immunization records to be used in aiding, coordinating, and promoting efficient and cost-effective childhood communicable disease prevention and control efforts, shall establish and maintain a childhood immunization registry."

The 78th Legislature (2003) passed House Bill (HB) 1921 to simplify reporting immunization histories to DSHS and enhance the effectiveness of the immunization registry; help populate the registry by relieving payors and providers of the responsibility for maintaining consent for the registry; allow parents to submit immunization histories directly to the department; require healthcare providers and payors to send immunization records directly to the department; require the department to verify parental consent for each record submitted; and expand data access to any provider authorized to administer vaccines, payors and state agencies with legal custody of a child. HB 1921 was fully implemented January 1, 2005. (Appendix A)

DSHS agency rules concerning the Texas immunization registry were approved by the Texas Board of Health in April, 2004 and became effective May 6, 2004. The rules may be found in the Texas Administrative Code, Title 25, Part I, Chapter 100. (Appendix A)

3. Registry Functional Standards

The Centers for Disease Control and Prevention (CDC) National Immunization Program adopted Registry Functional Standards recommended by the National Immunization Program's Technical Working Group (TWG) on May 15, 2001. The ImmTrac registry currently meets the following CDC Registry Functional Standards:

- ☑ Electronically store data on all National Vaccine Advisory Committee (NVAC) approved core data elements
- ☑ Enable access to and retrieval of immunization information in the registry at the time of encounter
- ☑ Receive and process immunization information within 1 month of vaccine administration
- ☑ Protect the confidentiality of health care information
- ☑ Ensure the security of health care information
- ☑ Automatically determines the routine childhood immunization(s) needed, in compliance with current ACIP recommendations, when an individual presents for a scheduled immunization
- ☑ Automatically identify individuals due/late for immunization(s) to enable the production of reminder/recall notifications
- ☑ Automatically produce immunization coverage reports by providers, age groups, and geographic areas
- ☑ Produce official immunization records
- ☑ Promote accuracy and completeness of registry data

An additional CDC Functional Standard is currently not being met, but efforts are ongoing to implement processes to meet this standard during 2005:

- ☐ Establish a registry record within 6 weeks of birth for each newborn child born in the catchment area

4. Data Management

The security, confidentiality, and privacy of children's information contained in ImmTrac are of utmost priority to the registry staff. The daily operation of the registry requires policies and procedures that address: security, data acquisition, timeliness of data entry, data quality, error correction, and consolidation of multiple records into a single record per individual. User education and training will be necessary on all these issues. ImmTrac staff sign confidentiality statements at employment, are trained to use ImmTrac and are allowed access to the various areas of the ImmTrac system as required by specific job tasks of the position.

The department may obtain the data constituting an immunization record for a child from:

- a public health district
- a local health department
- the child's parent
- a physician to the child
- a payor, or
- any health care provider licensed or otherwise authorized to administer vaccines.

The department may release the data constituting an immunization record for a child to any entity that is described above, and to:

- a school or child care facility in which the child is enrolled, or
- a state agency having legal custody of the child.

5. Registry Access

5.1 Registration

Sites wishing to access the registry must first register with DSHS and sign a memorandum of understanding and confidentiality statement (MOU) before being granted access to ImmTrac. ImmTrac security staff, through the appropriate Texas licensing/accreditation authority, to the extent possible verifies all registrations. The ImmTrac security manager creates groups of users and assigns the groups only the authority to perform the group appropriate operations. Each group is assigned certain access and report rights appropriate for their assigned group.

After receiving the required registration forms, ImmTrac staff will contact the site by e-mail or regular mail to provide additional instructions for printing the ImmTrac Instruction Manual and checking the Internet browser version. When the process has been completed, ImmTrac Customer Support is notified. At that time, ImmTrac Customer Support assigns a user id and calls the site contact person with a browser authentication code, user login credentials, and basic user training. Setup usually takes only a few minutes over the phone.

At registration the ImmTrac security manager assigns temporary passwords which application rules require the user to change on the first logon before accessing the system. During the installation appointment, authorized ImmTrac staff assigns limited-life codes to allow users to register for the ImmTrac Web.

Before a web user can log on, the user is instructed that they must read and agree to the on-line ImmTrac confidentiality agreement before being allowed to continue into the ImmTrac system. The user must click the “I agree” button before the application will allow them into the registry log on page. If the user does not agree to the Confidentiality Statement and clicks the “I disagree” button, the application denies access to the log on page and returns the user to the ImmTrac home/informational page.

5.2 Online access

Users authorized to access registry data through the online Internet application may perform client searches, view client immunization detail information, and print immunization histories. Authorized users may access the reporting features to generate Reminder and Recall reports, letters, and mailing labels. Additional online reports are available for users with appropriate security clearance. The Internet application features a user-friendly interface, screen tips, and a user instruction manual available online.

5.3 Immunization History Request Process

Health plans and payors may utilize the ImmTrac Immunization History Request Process (IHRP). This process allows a health plan to submit an electronic file containing a listing of health plan clients, including demographic information for matching purposes. ImmTrac staff will process the IHRP request file and return to the submitting entity an electronic file containing

the immunization history for clients found to match ImmTrac clients. Additional information is available in the Immunization History Request Process Document (Appendix A).

5.4 Paper Reporting

Providers who cannot meet the minimum computer system requirements for direct access to ImmTrac can submit client immunization information to ImmTrac using the ImmTrac Paper Reporting Form. Upon receiving the completed application forms for paper reporting, ImmTrac Customer Support staff mails the provider a reporting form packet containing an instruction page, reporting forms, continuation pages, and an ImmTrac consent form. Paper immunization histories and other paper forms sent by parents and providers are stored in a secured cabinet until entered into the registry by ImmTrac staff. After data entry, the forms are shredded, returned to the parent or provider, or stored in a locked cabinet.

6. System Security

6.1 Production Servers

All ImmTrac production servers are configured according to the DSHS network security policies and are located in a secured physical location with access strictly limited to authorized personnel. These servers are behind the DSHS firewall that restricts unauthorized access.

Production import functionality is granted to users on an as needed basis. Sites wishing to import to ImmTrac must register and obtain specific access rights from the security manager prior to importing test files. Imported files are linked to specific users and must adhere to strict file naming conventions.

6.2 Applications - Web ImmTrac

Web ImmTrac uses SSL and 128-bit encryption for all data transmitted over the Internet. Application access requires a user ID and password assigned by the ImmTrac security manager. ImmTrac employs password encryption, password naming restrictions, and password expirations. A user is locked out after a set number of unsuccessful login attempts. ImmTrac doesn't give specific messages that might identify the reason a user can't log in. The message does not differentiate between an unrecognized user ID and an incorrect password. Each login (or attempt to log in) is captured either in an error table or a login table that is reviewed daily. Idle accounts, those not accessed in 90 days, can be disabled.

ImmTrac staff provides the user with a registration code, that when entered, will give the user access to the confidentiality statement in order to logon to the ImmTrac system. Entry of the registration code creates a cookie with a predetermined expiration date. The cookie is stored within each individual user's profile on their PC.

6.3 Database

Database access requires a user ID and password separate from the application user ID and password and is limited to ImmTrac staff. Users are required to have specific authority,

assigned by the ImmTrac security manager, to perform database operations. ImmTrac includes an auditing feature that gives the ability to track record changes. Also, all tables contain fields that record the time and user ID of all record updates.

7. Data Quality

7.1 Adding New Clients – Data Entry

ImmTrac is an "opt-in" registry; written parental consent is required to include a child's immunization record in the registry. Consent must be given by the child's parent, legal guardian or managing conservator. DSHS is responsible for verifying parental consent before creating a new client immunization record. Providers are instructed to search the ImmTrac application to determine if a client is in the registry. If the client record is not located in ImmTrac, a consent form may be printed from the ImmTrac application. The consent form may be signed by the child's parent and faxed to ImmTrac for verification of consent and creation of the new client record.

Consent forms are received at a dedicated fax server located in the ImmTrac offices. The imaging system has a modem and server loaded with WinFax software to automatically receive faxes. Program staff review each consent form received to ensure it is legible; the information is complete, the consent box is checked and the form is signed by the parent, guardian or managing conservator. If the form does not meet these criteria, it is moved to an Issues folder for later resolution.

If the consent form is properly submitted, ImmTrac staff determines if the child listed on the consent form is already in ImmTrac. To try to locate the person, program staff will perform a Basic and Smart Search in ImmTrac. The ImmTrac Smart Search allows the user to enter additional client demographic information, and utilizes an intelligent matching algorithm to provide a greater chance of finding an existing ImmTrac client.

- During the search process, if the child is located and verified to match the information on the consent form, then consent was previously granted and the incoming image is not retained.

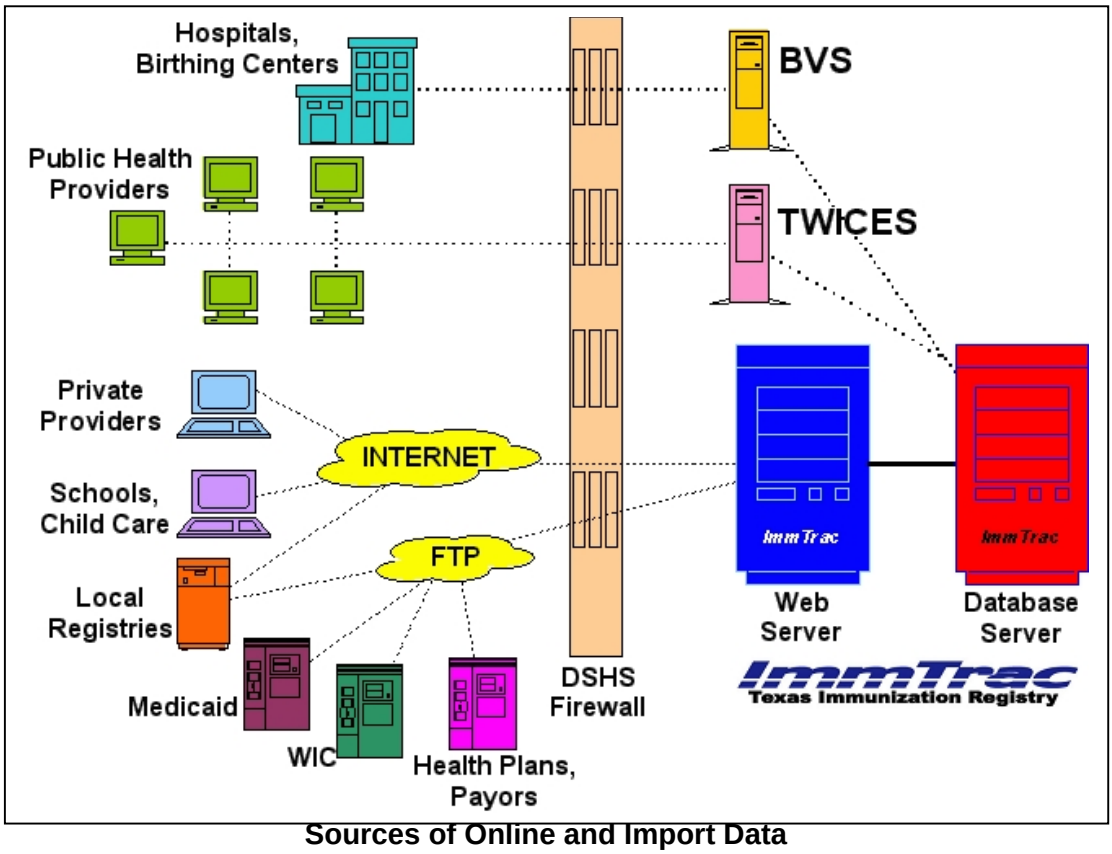
- If a match to an existing client cannot be found, the new client is added to ImmTrac using the information from the Smart Search (Name, Address, City, State, Zip, County, DOB, Name of Parent) to create a record. The consent image is indexed and retained as evidence of consent.

7.2 Data Import

Imported data represents the largest source of records for the registry, import editing and record validation is very important. Imported immunization data is received from numerous sources, including Vital Statistics (birth data), Medicaid, public health clinic client encounter data, provider groups and physicians networks, health plans and payors, and WIC clinics. DSHS has

established standard import file formats to control data quality and consistency. All payors and providers who choose to submit data electronically are required to use the appropriate *ImmTrac Electronic Transfer Standards* for data files sent for import into ImmTrac. (Appendix A)

Import files may be submitted to ImmTrac via secure encrypted FTP or by secure upload to the ImmTrac Internet application. Program staff works directly with data submitting entities to setup test files prior to allowing data sets to be imported into ImmTrac. Staff examines data files from sources prior to import for data accuracy and completeness and provides feedback on test files. Once files are imported, statistics are captured on each imported file. Statistics include errors in the import process. Program staff works with the importers to resolve the errors, to the extent possible.



Sources of Online and Import Data

The Import process edits the following information for validity and format:

- Client name
- Zip code and county of client address, if present
- Date of Birth
- Vaccine/Immunization code
- Immunization date is also edited against date of birth to ensure the date of service is not before the date of birth

Table editing performed during import is:

- All tables capture the first and last users and related dates
- Added records contain an identifier to identify a record as added via import and the date it was added;
- Edited records contain the date the record was modified and an identifier to indicate that the edit was caused by import
- Import error log captures: Import date; file name, import file record number; cause of error; database id number; and, if the record creates a QM (Questionable Match), the log captures the id number of the possible match
- Records added as QMs are identified by a flag

Data Review:

- Import error logs are reviewed for submitter issues and areas in which programmatic changes can improve data capture;
- In cases of submitter data digression, logs are printed for submitter reconciliation;
- Ad hoc data review to identify undisclosed issues in the error log due to data entry;

7.3 Editing

Online data entry has rigorous data requirements, e.g. address information is required to add new clients, and dates for immunizations are cross-checked to ensure they are equal to or later than the child's date of birth. To prevent duplicate client records on the database and to ensure that updates are applied to the correct records, the on-line add or data import must attempt to determine if an incoming record represents a client who is already on the database.

On client search, the system displays all possible client matches for reconciliation; confirmation of adds/edits is required prior to the user saving data. The ability to merge duplicate clients is limited to authorized individuals. Users other than registry staff are not allowed to delete client or immunization information. On all data adds and edits, the system captures the date and the id of the user making the change.

ImmTrac processing includes specific validation of client and immunization data before it is added to the registry during import. After import, staff monitors the various import statistics to detect and resolve data problems. Import error and Questionable Match rates are monitored to detect high rates or unusual fluctuations within a provider subset.

8. Client Matching in ImmTrac

8.1 Verification of Consent

State law requires that DSHS verify that parental consent has been granted prior to including a child's immunization record in the registry. Verification of consent is performed by electronic matching of an incoming record with the database of consent-verified clients. Incoming records matching an existing consent-verified client are updated with new immunization information. Incoming records that do not match an existing verified client are rejected and not entered into the registry database. State law prohibits DSHS from retaining individually identifiable information about clients for whom consent cannot be verified.

8.2 Client Matching

In an online add, a client list containing potential matches identified by ImmTrac's matching algorithm is presented to the user, who must then examine each of these potential match clients to determine if one of them might represent the client being added. If no match is found, the user is instructed to print the ImmTrac consent form and offer the parent the opportunity to grant consent for registry participation.

In the import process, if a match to an existing client record is found, the existing client record is updated with new information. If no match is found, the import record is rejected and no individually identifiable information about the client is retained. If a potential match is found, but the strength of the match (the match weight) is below a pre-defined threshold, the client is added to the database and flagged as a questionable match (QM). ImmTrac staff review QM clients added by import to determine whether they should remain unique or be merged with a client already on the database.

ImmTrac's client matching algorithm is used not only in the online add and import processes, but also by ImmTrac's standalone de-duplication process Automated Client Merge (ACM).

8.3 The Matching Process

ImmTrac's matching process consists of three main steps: standardization, search and comparison. Each of these steps produces a specific result that is then used by the following step.

Standardization

The first step in the matching process is to standardize data from the incoming record. This is performed by the matching algorithm standardization process, and involves applying a set of rules that convert incoming raw data to consistent values, e.g. Bob is converted to Robert, and 123 Main Street is converted to 123 Main St.

Searching for Potential Matches

The second step in the matching process involves searching the database for clients that we think might be potential matches to the incoming client from either an import record or an on-line add. For each incoming client, ImmTrac's matching algorithm makes up to three passes searching for potential matches. After each pass, the third step in the matching process is performed: calculating the match weight. Each pass in the search for potential matches uses one or more pieces of client information to bring back a list of existing clients that have the same values in the those fields.

Search Passes

- Pass One, designed to quickly catch easily matched records, uses the SSN field to query the database for any client records with the same SSN If the SSN field is blank on an incoming record, pass one is skipped. About one-third of the client records on the database contain values for the SSN field.

- Pass Two searches primarily on last name, and it is where most of the matches will occur. To tolerate some variation in the spelling of the last name, this pass uses the NYSIIS code of the last name, rather than the last name itself. This allows us to find potential matches with differences in last name spellings, such as “Smith”, “Smyth” and “Smithe”, for evaluation in the comparison step. Searching on NYSIIS code of last name, gender, birth year and birth month, this pass is much more inclusive than Pass One. Passes One and Two together cover the major fields which are available for a client, and which are accurate and stable - SSN, last name, gender and date of birth. Unless these fields are incorrect, only last name is subject to change, and such changes should be infrequent.
- Pass Three serves as a safety net to find potential matches that were not found in either of the earlier passes because of incorrect or missing data fields. This pass searches using mainly address information. The search fields are NYSIIS code of street name, the street number with the two least significant (rightmost) digits truncated, the first three digits of the zip code and the birthday.

If ImmTrac’s three-pass approach fails to find any potential matches for an incoming client, or those that are found don’t have a high enough match weight to be considered QMs, this indicates that the incoming client has unique values in enough major fields that even a comparison against every record on the database would most likely not find a match.

8.4 Comparison - Calculating Match Weight

The final step in the matching process involves comparing a pair of records and calculating a total match weight based on how well the data in each matches. After each pass, the matching algorithm compares every member of the potential match list to the incoming record and calculates a match weight for that pair. ImmTrac then compares the total match weight for the pair to pre-defined cutoff weights to determine if the incoming client represents a duplicate to an existing client, a QM or a unique client.

To calculate the match weight, the ImmTrac matching algorithm adds or deducts points for each field in a record pair depending on whether the field values agree or disagree. If a value is missing in either record, points are neither added nor deducted for that field. When all fields have been analyzed, the field points are added together to arrive at the total match weight. Based on the match weight, the existing/incoming pair is labeled a definite match, a definite non-match (unique) or a QM.

Types of QMs

- Clerical QM-This indicates that the matching algorithm is unsure whether the records in the pair are the same and that clerical review is necessary.
- Birth Date QM-This indicates that the matching algorithm declared the pair a match, but that the dates of birth on the incoming and existing records are not exactly the same. Since this field is used to evaluate and recommend a child’s shot schedule, and since we have no way of knowing which of the two dates of birth is correct, we flag the incoming record as a QM. Birth date QMs are often siblings.
- First Name QM-This indicates that the matching algorithm declared the pair a match, but that the standardized first names are not exactly the same. We flag a QM in this situation to prevent merging twins, with the same data in all fields except the first name and possibly middle names the same, into a single child on the database. First Name QMs are often twins.
- Gender QM-This indicates that the matching algorithm declared the pair a match, but that the genders on the incoming and existing records do not agree. We flag a QM in this

situation to force a manual review and determination of the correct gender of the child. Gender QMs often represent incorrect data.

8.5 AutoMatch

AutoMatch is a standalone program that attempts to link, or match, records on two input files or to find duplicate records on a single input file. AutoMatch adds or deducts points for each field in each record of a potential record pair depending on whether the field values agree or disagree. If a value is missing on either record the field receives no points. When all fields have been analyzed, the field points are added together to arrive at the strength of the match. Based on the number of points for the records, the record pair is labeled a definite match, a definite non-match (unique), or a clerical match. A clerical match indicates that the software is unsure whether the records in the pair represent the same client, and that staff review is necessary to make the determination.

8.6 Automated Client Merge (ACM)

ImmTrac also includes separate functional modules that detects duplicate clients in a flat file created from the client table and produces a file of duplicate client identification information which can be used as input to the Automated Client Merge (ACM) program. This module also uses matching algorithm deduplication.

Automated Client Merge (ACM) is a separate functional module/de-duplication process that is run periodically to identify multiple existing ImmTrac records that represent the same child. Those records that cannot be resolved automatically by the process are flagged as Questionable Match (QM), while those that are determined to be duplicates are merged into a single record with a combined immunization history.

9. Data Backup and Archive

9.1 Backup Schedule

Technical staff backs up the database to disk on weeknights Monday through Friday. Staff backs up and clears out the transaction log, a file that records changes to the database, to disk mid-day and also on weeknights before the database backup. DSHS IT operators back up these disk files to tape several times each week, and store backups under controlled conditions according to DSHS IT retention guidelines.

9.2 Archive

ImmTrac uses an automated process that removes any records and linked immunizations that pertain to over age clients (older than 18 years of age). This process is scheduled and run periodically.

Appendix A

Relevant Links:

Annual Report on Plans to Increase Immunization Rates in Texas:
http://www.tdh.state.tx.us/immunize/docs/2004_Ann_Rept.pdf

House Bill 1921:
http://www.tdh.state.tx.us/immunize/docs/Payors/HB1921.pdf

DSHS Rules Concerning the Texas Immunization Registry:
http://www.tdh.state.tx.us/immunize/docs/Payors/ImmTrac_rules.pdf

Key Changes Required for Implementation of HB 1921:
http://www.tdh.state.tx.us/immunize/docs/HB1921.pdf

Electronic Transfer Standards for Payors:
http://www.tdh.state.tx.us/immunize/docs/Payors/EFT_standards.pdf

Electronic Transfer Standards for Immunization History Request Process (IHRP):
http://www.tdh.state.tx.us/immunize/docs/Payors/ImmTrac_Electronic_Transfer.pdf

Appendix B

Revision History:

Version	Date Published	Author	Phone	Changes
Version 1.01	01/25/2005	Ann Grizzard	(512) 458-7111	Initial version of document created
Version 1.02	02/11/2005			Add additional information on Matching,
Version 1.03	03/01/2005			Include comments from L Davis & K. Allen
Version 1.032	04/01/2005	Lola Davis and Cynthia Pryor		Update and edit contents. This includes updates from T. Veach and L. Creagh.
Version 1.04	04/05/2005	Claude Longoria		Review and edit.