The Tuberculosis Control Program (TBCP) of County of Los Angeles (LAC) Department of Public Health (DPH) submits this Data Management Plan in compliance with the terms of and activities expected by the Centers for Disease Control and Prevention (CDC) under the Notice of Funding Opportunity (NOFO) CDC-RFA-PS20-2001.

# DESCRIPTION OF DATA COLLECTED AND GENERATED THROUGH PROGRAMMATIC ACTIVITIES

## Tuberculosis Registry Information Management System (TRIMS)

TRIMS is a mission-critical surveillance system developed by the TBCP to collect and report data pertaining to the incidence and prevalence of TB disease, the evaluation of contacts, and the evaluation of target populations for Latent TB Infection (LTBI) in LAC. Core functions of the TBCP and other entities within DPH are supported through TRIMS. The CDC and California Department of Public Health (CDPH) mandate the reporting of all TB cases, and TRIMS produces a Report of Verified Case of Tuberculosis (RVCT) data record and facsimile output report. TRIMS is the system of record from which epidemiological statistics are generated for annual progress reports to the CDC, including performance measures based on the National TB Indicators Project (NTIP) and the Aggregate Report for Program Evaluation – Contact Investigations (ARPE-CI). TRIMS is designed to support these reporting requirements and provides a platform for the collection of additional information specific to LAC. A patient record created TRIMS remains there indefinitely, allowing TBCP to track a patient from initial screening through confirmation of TB disease, in addition to storing multiple evaluations for TB infection or TB disease over many years.

## Case Management and Processing System (CMaP)

CMaP is a case management system used by the district health nurses to manage TB case investigations and contact investigations and to measure performance indicators related to contact investigations. Beginning in 2018, CMaP became the source record for contact evaluation data. The TBCP extracts these data and combines it with TB case date extracted from TRIMS to produce the ARPE-CI report.

## California Reportable Disease Information Exchange (CalREDIE) System

The TBCP, in addition to other DPH disease control programs, is required by the California Department of Public Health (CDPH) – TB Control Branch (TBCB) to manually enter all RVCT records into CalREDIE to fulfill mandated TB case reporting requirements of the State of California. The DPH is negotiating with CDPH to re-establish electronic reporting of RVCT data to CalREDIE, which CDPH stopped supporting in calendar year 2011. At a minimum, the TBCP would prefer to provide CDPH with an electronic file exchanged through a Secure FTP Server site which can imported into CalREDIE via an Ad Hoc Import feature in CalREDIE. The DPH maintains a CalREDIE Data Use and Disclosure Agreement with CDPH.

## Integrated Reporting, Investigation, and Surveillance System (IRIS)

The DPH is currently developing IRIS as a single integrated public health surveillance system to be used by all disease control programs, replacing the functionality currently built out in TRIMS and CMaP. IRIS is being built to meet operational needs of the DPH, and functionalities will include electronic laboratory and notifiable disease reporting, case management, contact investigation, genotype cluster investigation, and surveillance of LTBI. The system will be able to generate RVCT, ARPE-CI, ARPE-TT, and NTIP data records and output reports.

## TB Patient Interview Database

The TBCP Genotype Cluster Investigation and Assessment (GCIA) team provides an in-depth patient interview service to support District Public Health Nursing case management and contact investigation activities. Each patient interview is stored in a dedicated Microsoft Access database on a secured Microsoft Active Directory Services network share drive managed by the DPH Information Systems Division (PHIS).

## Contact Investigation and Outbreak (CIOB) Database

The TBCP GCIA team and CIOB team store summary data about high-priority contact investigations in a dedicated Microsoft Access database on a secured Microsoft Active Directory Services network share drive managed by PHIS.

## Laboratory data

Public Health Laboratory (PHL) test results are stored in a vendor-based accessioning system and backup data is warehoused and maintained in a database at PHL. PHL deployed an automated system whereby test results, in text file format, are saved to a secured Microsoft Active Directory network shared folder. TBCP uses the CDC-TB-GIMS application to submit information and TB isolates for genotyping service, and to receive genotype results. Currently, the TBCP imports the genotype results into TRIMS and populates a special form within the patient’s Incident record.

## Fax Server (RightFax)

In 2018, the TBCP implemented an electronic fax server solution to replace the previous paper-based fax workflow for receiving notifiable disease reports from laboratories and health care providers. Implementation of the fax server solution transformed the process of sharing secure information between the TBCP, public health districts, and the community while minimizing paper consumption and improving workflow efficiency and staff productivity. In addition to providing an added layer of data security for patient information, the fax server solution is a critical component for the TBCP Continuity of Operations Plan (COOP) by ensuring the delivery of essential services to the public and other government agencies in the event of a disaster situation where access to the TBCP office facility is prohibited. The fax server is accessible via a secure HIPAA compliant connection to the DPH information system infrastructure from any internet access point. TBCP personnel can work from other County facilities or telework during a disaster situation. The data collected via RightFax includes notifiable disease reports, case management and contact investigation information, some of which is eventually reported to the CDC to meet mandated reporting requirements.

## Online Real-time Centralized Health Information Database (ORCHID)

The DPH and the Department of Health Services deliver outpatient and inpatient TB-related healthcare services. Both departments use an Electronic Health Record system called ORCHID to document patient encounters, including all diagnostic testing and treatment of the patient. The TBCP Liaison Public Health Nurses assigned to the DHS County hospitals and Jail medical service facilities collect information from ORCHID and store this information in TRIMS to support public health surveillance activities. Similarly, DPH District Public Health Nursing collects information from ORCHID and stores this information in TRIMS and in CMaP to support public health surveillance activities. In the future, ORCHID information will be exchanged electronically with IRIS to support public health surveillance activities.

# Data retention

The TBCP complies with the DPH and LAC policies pertaining to records retention, these are:

* DPH Policy No. 343 Records Management Program
* DPH Policy No. 343-I LAC General & Departmental Records Retention Schedules
* DPH Policy No. 343-II Departmental Records Retention Schedule

All data generated by and entered into the aforementioned databases will be retained perpetually. Laboratory data and reports are retained per regulatory requirements from CDPH Clinical Laboratory and Evaluation Program and Environmental Laboratory Accreditation Program and per LAC’s Records Retention Schedules.

# Data format

TRIMS is a SQL server backend database and the application uses classic ASP pages for the front-end user interface. Both the SQL server and the web server are housed in the PHIS data center. TRIMS is an intranet-based application and originated as a mainframe application from which the data was imported. Data is extracted from the SQL databases are saved in SAS datasets, Excel files, or Access databases. Supplementary data are stored in a Microsoft Access database housed on a secured Microsoft Active Directory network share folder managed by PHIS.

# Data sharing

Sharing and dissemination of data are governed by the LAC Countywide Data Sharing Handbook. The handbook provides guidance to all departments on appropriate data sharing, including sharing of legally protected information. Terms include term limits, de-identification procedure of data, HIPAA language, data security plan, and indemnification language. Public requests for data are granted after completion of the data use agreement. De-identification of data will be performed for files to be submitted to CDC.

# Data security

The DPH provides guidance on data security policies and procedures. Data security procedures comply with the security requirements of all applicable regulatory, compliance, and accreditation sources to secure all electronic data including Protected Health Information (PHI) and other confidential information, including HIPAA protected health information. Confidentiality, integrity, and availability of information assets are protected from unauthorized disclosure, modification, or destruction and safeguarded to the extent permitted by law. Workforce members involved with data comply with the provisions of all relevant data security policies and procedures. Users are to immediately report any and all suspected breaches of information security and comply with all required security training within the required timeframes. Information assets are limited only to those persons with documented business needs and access authorization. System Managers implement appropriate technical access control safeguards via system activity logging, unique user identification, authentication, approval-based provisions, and rule-based provisions.

# Archiving and long-term preservation

PHIS built and currently hosts a centralized data repository for existing DPH source systems, including TRIMS. The repository is used data analytics, trend analysis, measurement of program performance indicators based on NTIP, and generation of surveillance reports and the annual CDC progress report. Data is stored in a SQL server, refreshed daily, and retained perpetually. Other external and routinely used databases and ones associated with publications are archived and preserved in a secured Microsoft Active Directory Services network share folder managed by PHIS.

# INFORMATION TECHNOLOGY & DATA SECURITY and CONFIDENTIALITY POLICIES

The DPH maintains an extensive set of policies pertaining to the use of information technology systems, including a number of data security and confidentiality policies, related to the systems described above in Section I. ~~A copy of any of the following policies, or policies described in the sections above, are available upon request.~~ A copy of any of the information technology, data security and confidentiality policies related to the systems described above and their use is available upon request.

## POLICY SERIES 1000: INFORMATION TECHNOLOGY

* Policy No. 1000 Public Health Information Technology and Security Policy
* Policy No. 1000 Attachment I – Information System Glossary
* Policy No. 1001 Security Management Process – Risk Management Policy
* Policy No. 1002 Workforce Security Policy
* Policy No. 1003 Information Access Management Policy
* Policy No. 1004 Security Incident Report and Response Policy
* Policy No. 1005 Facility/Program Information Technology (IT) Contingency Plan Policy
* Policy No. 1006 Security Compliance Evaluation Policy
* Policy No. 1007 Facility Access Control Policy
* Policy No. 1008 Workstation Use and Security
* Policy No. 1009 Device and Media Control Policy
* Policy No. 1010 System Access Control
* Policy No. 1011 Public Health System Audit Controls
* Policy No. 1012 Information Integrity
* Policy No. 1013 Person or Entity Authentication
* Policy No. 1014 Data Transmission Security
* Policy No. 1015 Data Security Documentation Requirement
* Policy No. 1016 Acceptable Use Policy for County Information Technology Resources
* Policy No. 1016 Attachment I – Annual Agreement for Acceptable Use and Confidentiality of County Information Technology Resources
* Policy No. 1017 Departmental Computer Configuration Standards Compliance
* Policy No. 1030 Information Technology Purchases
* Policy No. 1031 Administration of Public Health Data Network
* Policy No. 1032 Information Technology Budget Requests/Adjustments, Grant Applications, and Grant Budget Adjustments
* Policy No. 1033 Electronic Mail (EMAIL) Retention

## POLICY SERIES 1200: HIPAA (HEALTH INSURANCE PORTABILITY AND PRIVACY ACT)

* Policy No. 1201 Privacy and Security Compliance Program
* Policy No. 1202 Notice of Privacy Practices
* Policy No. 1202 Attachment I – Notice of Privacy Practices
* Policy No. 1202 Attachment II – Acknowledgement of Receipt Form
* Policy No. 1203 Use and Disclosure of Protected Health Information Without Authorization
* Policy No. 1204 Uses and Disclosures of Protected Health Information (PHI) Requiring Authorization
* Policy No. 1205 Right to Request Restrictions on the Uses and Disclosures of Protected Health Information (PHI)
* Policy No. 1206 Right to Request Confidential Communications of Protected Health Information (PHI)
* Policy No. 1207 Opportunity for an Individual to Agree or Object to the Use and Disclosure of Certain Protected Health Information
* Policy No. 1208 Minimum Necessary Requirements for Uses and Disclosures of Protected Health Information (PHI)
* Policy No. 1209 Incident Uses and Disclosure of Protect Health Information (PHI)
* Policy No. 1210 Disciplinary Actions/Sanctions for Failure to Comply with Privacy Policies and Procedures
* Policy No. 1211 Complaints Related to the Privacy of Protected Health Information (PHI)
* Policy No. 1211 Attachment I – Breach of Protected Health Information Risk Assessment Tool
* Policy No. 1212 Waiver of Rights
* Policy No. 1213 Non-Retaliation
* Policy No. 1214 Designated Record Set
* Policy No. 1215 Access of Individuals to Protected Health Information (PHI) Designated Record Set

Attachment A – Patient’s Request for Access to Health Information

Attachment B – Letter Responding to Request for Access to PHI

Attachment C – Request for Review of Denial of Access to PHI

Attachment D – Final Letter of Response for Review of Denial to Access to PHI

* Policy No. 1216 Verification of Identify and Authority of Individuals Requesting Protected Health Information
* Policy No. 1217 Use and Disclosure of Protected Health Information of Deceased Individuals and Minors Making Disclosure to Personal Representatives
* Policy No. 1218 Amendment of Protected Health Information (PHI) Designated Record Set
* Policy No. 1219 De-Identification of Protect Health Information/Limited Data Sets
* Policy No. 1220 Business Associate Agreement

Attachment A – Business Associate Agreement under HIPAA

Attachment B – Compliance with HIPAA of 1996 – Providers of Patient Care Services

Attachment C – Inadvertent Medical Record Access

* Policy No. 1221 Accounting of Disclosures
* Policy No. 1222 Implementing Changes to Privacy Policies
* Policy No. 1223 Safeguards of Protected Health Information (PHI)
* Policy No. 1224 Privacy and Security Awareness Training
* Policy No. 1225 Disclosure of Protected Health Information (PHI) by Whistleblowers Without Patient’s Authorization
* Policy No. 1226 Mitigation
* Policy No. 1227 Use and Disclosure of Protected Health Information for Research Purposes
* Policy No. 1228 Use and Disclosure of Protected Health Information for Fundraising
* Policy No. 1229 Use and Disclosure of Protected Health Information for Marketing Purposes
* Policy No. 1230 Disclosure of Protected Health Information (PHI) by Workforce Crime Victims Without Patient’s Authorization
* Policy No. 1231 Disclosure of Protected Health Information (PHI) Without Patient’s Authorization for Public Health Activities
* Policy No. 1232 Permitted Uses and Disclosures of Protected Health Information for Treatment, Payment, or Health Care Operations Without Patient Authorization
* Policy No. 1233 Disclosure of Patient’s Protected Health Information (PHI) to His or Her Family Member, Close Personal Friend, or Personal Representative Without Authorization
* Policy No. 1234 Permitted Uses and Disclosures of Protected Health Information for Law Enforcement Requests Without Authorization
* Policy No. 1235 Permitted Uses and Disclosures of Protected Health Information for Court Order and Subpoena Requests
* Policy No. 1236 Privacy & Security Breach Notification Policy

Attachment A – Breach of Protected Health/Personal Information Risk Assessment Tool

Attachment B – Information Security Incident Report

Attachment C – Unsecured Protected Health/Personal Information Breach Reporting Form