

Los Angeles County Department of Mental Health
**Integration Services
Provider Directory API
Policy and Procedures**

Version 1.0

Revision History

Date	Version	Description	Author
09-30-2024	1.0	Initial Draft	DMH Integration Services Team

Sign Off

Date	Signatory Name	Initials

DRAFT

Table of Contents

REVISION HISTORY	2
SIGN OFF	2
TABLE OF CONTENTS	3
PROVIDER DIRECTORY API POLICY AND PROCEDURES	4
1.0 PURPOSE	4
2.0 POLICY	4
2.1 DATA AVAILABILITY	4
2.1.1 Data Accuracy	4
2.1.2 Data Access	5
2.1.3 Update Tracking	5
2.2 TESTING & MONITORING EVIDENCE	5
2.2.1 Routine Testing	5
2.2.2 Monitoring Evidence	5
2.2.3 Review	6
3.0 PROCEDURES	6
3.1 DATA AVAILABILITY	6
3.1.1 Data Access	6
3.1.2 Data Accuracy	7
3.1.3 Update Tracking	7
3.1.4 Information Updates	7
3.2 TESTING & MONITORING EVIDENCE	7
3.2.1 Routine Testing	7
3.2.2 Monitoring Evidence	7
3.2.3 Reporting to DHCS	8
3.2.4 Monitoring and Review	8
4.0 AUTHORITIES	8
5.0 REFERENCES	8

Provider Directory API Policy and Procedures

1.0 Purpose

Los Angeles County Department of Mental Health (DMH) maintains a comprehensive provider directory API containing information for all healthcare practitioners of DMH directly operated and contracted network of providers. This policy and procedures document outlines the implementation, compliance, and operational guidelines for Behavioral Health Information Notice No: 22-068 and Behavioral Health Information Notice No: 23-032 related to the Provider Directory API requirements.

This document ensures compliance with DHCS and CMS standards for behavioral health services, including procedures for maintaining an accurate and updated provider directory via the API. It provides guidelines for the timely availability of provider data, updates within 30 days, and evidence for testing and monitoring API compliance.

All personnel must follow these policies and procedures to maintain accuracy, availability, and timely updates in the Provider Directory API and ensure compliance with DHCS and CMS standards.

2.0 Policy

2.1 Data Availability

The Provider Directory API shall ensure timely and accurate availability of provider data to comply with DHCS and CMS requirements. All provider data shall be updated to reflect current availability and service capabilities.

All supplemental information on the syntax, data fields, and resources is available through the Provider Directory API Companion Guide published by the Department and the HL7 FHIR website (<https://www.hl7.org/fhir/R4/>).

2.1.1 Data Accuracy

All data made available through the API shall be updated no later than 30 calendar days after receiving new or corrected information. This ensures that the directory remains accurate and reliable for users.

2.1.2 Data Access

The API shall provide 24/7 access and include detailed documentation covering:

- API syntax, function names, required and optional parameters, data types, return variables, structures, exceptions, and error-handling methods.
- The software components and configurations required to interact with the API successfully.
- All technical requirements necessary for an application to be registered with any authorization server(s) deployed alongside the API.

The Department may collect identifiable information, such as IP addresses, user-agent strings, and application IDs, from users or applications accessing the API. This data is collected to prevent misuse, enhance security, and optimize system performance.

2.1.3 Update Tracking

The API shall track updates to provider information, including logging when new data is received or when corrections are required. The records will be updated with a timestamp of the last modification, and system logging will capture all update activity.

2.2 Testing & Monitoring Evidence

The Department shall regularly test and monitor the Provider Directory API for performance, security and compliance.

2.2.1 Routine Testing

The Department shall conduct routine API functionality testing through automated DevOps pipelines. Testing will occur after code check-ins and deployments, as well as during monthly scheduled maintenance.

2.2.2 Monitoring Evidence

The API shall collect usage data, error rates, and other performance tracking information to serve as evidence of compliance with State and federal requirements. Monitoring will be conducted using cloud monitoring tools to ensure the API is functioning and available to users.

2.2.3 Review

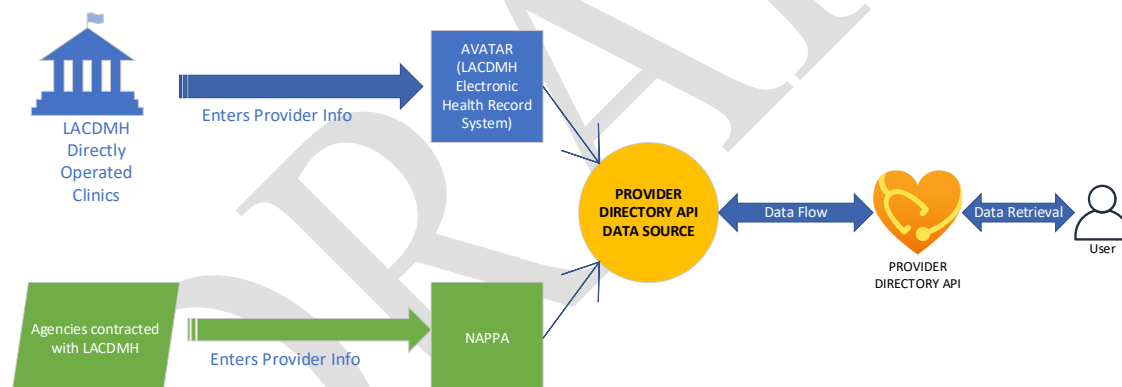
This policy will be reviewed annually or as necessary to account for changes in DHCS or CMS regulations.

3.0 Procedures

3.1 Data Availability

Provider network data is collected during the initial onboarding of each provider through the Department’s Electronic Health Record (EHR) system and the Network Adequacy Provider and Practitioner Administration (NAPPA) application. Updates are primarily handled through NAPPA, with data verified and processed by data warehouse integration jobs. Technical details on this application is available at DMH’s website.

Below is a diagram illustrating the data flow:



3.1.1 Data Access

This system will update records in alignment with monthly synchronization schedules between the EHR, NAPPA, and the API. The jobs will be logged and included as part of the quarterly audit. Reports will be available at request of IT compliance and security teams.

3.1.2 Data Accuracy

Provider data will be reviewed weekly to ensure accuracy, with updates processed regularly to maintain up-to-date information. Monthly data integrity checks will verify that the API accurately reflects provider information.

3.1.3 Update Tracking

A tracking system will log all updates, capturing the date and time when new information is received or corrected. An internal alert system will notify relevant teams when the synchronization job is not functioning.

3.1.4 Information Updates

The DMH Integration Team will process all updates in the provider database and push them to the API. Monthly checks will verify that updates are processed in a timely manner, ensuring compliance with the 30-day rule.

3.2 Testing & Monitoring Evidence

To comply with the CMS Interoperability and Access Final Rule, the Department will regularly test and monitor the Provider Directory API.

3.2.1 Routine Testing

Automated testing pipelines are used to verify the functionality of the APIs after code check-ins and deployments. Testing includes API availability, accuracy, and response time checks using Postman and PowerShell. Maintenance is scheduled monthly to ensure continuous functionality.

3.2.2 Monitoring Evidence

Weekly performance logs will be generated to track API uptime, error rates, and response times. These logs will be stored and reviewed to ensure the APIs are compliant with DHCS and CMS standards. A quarterly compliance report, including test results, monitoring logs, and any corrective actions, will be submitted to DHCS.

3.2.3 Reporting to DHCS

The compliance officer will prepare and submit evidence of testing and monitoring every quarter, including detailed information on testing methodology, monitoring processes, and corrective actions taken in the case of non-compliance.

3.2.4 Monitoring and Review

This policy will be reviewed annually or in response to updates from DHCS or CMS. Regular audits, performed as part of the quarterly review process, will ensure ongoing compliance.

4.0 Authorities

California State DHCS BHIN 22-068

<https://www.dhcs.ca.gov/Documents/BHIN-22-068-Interoperability-and-Patient-Access-Final-Rule.pdf>

California State DHCS BHIN 23-032

<https://www.dhcs.ca.gov/Documents/BHIN-23-032-Interoperability-Patient-Access-Final-Rule-Compliance-Monitoring-Process.pdf>

[CMS Interoperability and Access Final Rule](#)

5.0 References

Fast Healthcare Interoperability Resources (FHIR)

<https://www.hl7.org/fhir/overview.html>