LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

Los Angeles County Department of Mental Health

Integration Services
Patient Access API
Policy and Procedures

Version 1.0

Revision History

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

Sign Off

Date	Signatory Name	Initials

Table of Contents

LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

Patient Access API Policy and Procedures

1.0 Purpose

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, focusing on the Patient Access API. This API is critical for ensuring that patients can securely access their behavioral health information in compliance with state and federal mandates, including the CMS Interoperability and Access Final Rule.

The purpose of this document is to ensure timely, secure, and reliable access to patient health data, enabling patients to manage and share their healthcare information as needed, in accordance with DHCS requirements and CMS interoperability standards.

2.0 Policy

2.1 Data Availability

The Patient Access API shall ensure that patient health data is made available within one business day of receipt of the information or within one business day after the adjudication of a claim or receipt of encounter data, for dates of service on or after January 1, 2016, in compliance with state and federal regulations.

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

2.1.1 Data Accuracy

DMH shall validate and process all inbound source data to ensure data integrity and accuracy. Systems must be configured to synchronize new data with the Patient Access API automatically, ensuring that updates are reflected in real time for users.

2.1.2 Data Access

The API shall provide 24/7 secure access to patient health data, including:

- Patient care records, test results, medications, and treatment plans.
- Documentation on API syntax, function names, required and optional parameters, data types, return variables, error-handling methods, and structures.
- Information necessary for patients or third-party applications to securely connect to the API, including registration with any authorization servers as required.

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 patient 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 Third-Party Application Access and Security Risk Assessment

The Department reserves the right to deny or discontinue any third-party application’s connection to the API if it reasonably determines that continued access presents an unacceptable level of risk to the security of protected health information (PHI) based on the HIPAA Security Rule.

2.2.1 Security Risk Assessment

The Department will conduct a security risk analysis in compliance with the HIPAA Security Rule to assess whether third-party applications pose an unacceptable risk to the confidentiality, integrity, or availability of PHI. Applications that fail to meet the necessary security standards will be denied access to the API.

2.2.2 Denial or Discontinuation of Access

If a security risk is identified, the following procedures will be followed:

- Initial Notification: The third-party application provider will be notified in writing of the identified security risk.
- Temporary Suspension: Access to the API may be temporarily suspended while the risk is evaluated and corrective measures are taken.
- Permanent Denial/Discontinuation: If the risk cannot be mitigated, the Department may permanently deny or discontinue the third-party application's access to the API. The decision will be documented, and the provider will be informed of the reason for denial or discontinuation.
- Appeal Process: The third-party application provider may appeal the decision, submitting a corrective action plan to mitigate the identified risk.

2.2.3 Security Controls

Rate limits, encryption, and other security controls will be applied to all third-party applications accessing the API to ensure that no application compromises the security of PHI. Continuous monitoring will be performed to identify any potential misuse or unauthorized access.

2.3 Testing & Monitoring Evidence

The Department shall regularly test and monitor the Patient Access API for performance, security and compliance.

2.3.1 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.

2.3.2 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.

2.3.3 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

Patient health data is collected through the Department's Electronic Health Record (EHR) system. Updates, corrections, or additions to patient records are synchronized with the Patient Access API through scheduled data integration processes.

The API must reflect new or corrected patient data within one business day of receipt. This includes data from claims adjudication or encounter data for dates of service starting on or after January 1, 2016. Automated processes will ensure that data is synchronized and available to users within the one-business-day timeframe.

3.1.1 Data Access

This system will update records in alignment with daily synchronization schedules between the EHR 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

Patient 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 Patient 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 Integration Team will process all updates in the Patient database and push them to the API. Monthly checks will verify that updates are processed in a timely manner, ensuring compliance.

3.2 Third-Party Application Access and Security Risk Management

3.2.1 Security Risk Analysis

A security risk analysis and other onboarding processes will be performed for all third-party applications that request access to the API. This analysis will assess potential risks to the confidentiality, integrity, and availability of PHI and will follow the HIPAA Security Rule guidelines.

3.2.2 Application Denial or Discontinuation Process

- Identification of Risk: If an application poses a security risk, it will be temporarily suspended from accessing the API while the risk is reviewed.
- Notification: The third-party provider will be notified of the issue and provided with recommendations for mitigating the risk.
- Corrective Measures: The provider may submit a plan to address the risk. If the risk is mitigated, access may be restored.
- Permanent Denial: If the provider fails to mitigate the risk, access to the API may be permanently denied, and documentation of the denial will be submitted to DHCS.

3.2.3 Security Monitoring and Controls

Rate limits and continuous monitoring will be implemented to ensure that third-party applications do not overuse or misuse the API. Any application exhibiting unusual behavior will be flagged and investigated to prevent potential security breaches.

3.3 Testing & Monitoring Evidence

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

3.3.1 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.

3.3.2 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.

3.3.3 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.

3.3.4 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

- 42 CFR §431.60(a)
- 42 CFR §431.60(b)(1-4)
- 42 CFR §431.60(c)(2)
- 42 CFR §431.60(d)(1-3)
- 42 CFR §431.60(e)(1-2)
- 42 CFR §431.60(f)(1-2)
- 42 CFR §431.60(g)(1)
- 42 CFR §431.70(a-b)
- 42 CFR §438.242(b)(3-4

5.0 References

Fast Healthcare Interoperability Resources (FHIR)
https://www.hl7.org/fhir/overview.html