Health Care Agency **Behavioral Health Services** **Policies and Procedures**	Section Name: Sub Section: Section Number: Policy Status:	Client's Rights Member Access 02.07.01 ☒New ☐Revised

	SIGNATURE	DATE APPROVED
Deputy Director Behavioral Health Services	Signature on File	02/05/2026

SUBJECT: BHP Member Access to Application Programming Interface (API)

PURPOSE:

To outline the process for a Behavioral Health Plan (BHP) member to access service-related data in a timely manner, including a publicly accessible link or web URL where the Member Access Application Programming Interface (API) documentation is located, and to describe the process used by the BHP to deny or discontinue any third-party application's connection to an API.

POLICY:

I. It is the policy of Behavioral Health Services (BHS) to make available via an API encounter data within one business day after a claim is adjudicated and to make API access information publicly available on its website.

II. BHP reserves the right to deny or revoke third-party access to its Patient Access API if a documented security risk analysis identifies an unacceptable risk to PHI.

III. Health Care Agency (HCA) has implemented Oracle Health's FHIR/API solution, which enables timely patient data access through standards-based infrastructure and integration with national health information networks.

IV. HCA shall regularly test and monitor the Patient Access API to ensure compliance with CMS regulations, maintain system performance, ensure technical standards, and respond proactively to changes, issues, or outages.

SCOPE:

This policy applies to all Behavioral Health Plan members and clients served by BHS.

REFERENCES:

BHIN 23-032 Interoperability and Patient Access Final Rule Compliance Monitoring Process.pdf

DEFINITIONS:

Application Programming Interface – A set of rules that allows different software programs to communicate with each other.

Member – A person with Medi-Cal coverage who is served by the Orange County Behavioral Health Plan

PROCEDURE:

I. Member Access API Documentation

A. All information related to access shall be provided on a publicly available website.

II. Risk Management

A. The BHP reserves the right to deny or discontinue access to its Patient Access API by any third-party application if it reasonably determines, through a documented security risk analysis, that continued access poses an unacceptable risk to PHI.

B. Risk Identification and Assessment

1. The BHP shall monitor API activity and conduct periodic and event-driven security risk assessments. Indicators of risk may include:
    a) Unusual or excessive data requests
    b) Known vulnerabilities in the third-party app
    c) Reports of data breaches or misuse
    d) Failure to comply with authentication protocols

2. The risk shall be evaluated using the BHP's HIPAA-compliant risk analysis framework. The evaluation shall consider:
    a) Likelihood and impact of a breach
    b) Nature of the PHI at risk
    c) Mitigation measures available

3. If the risk is deemed unacceptable, the BHP shall:
    a) Document the findings and rationale
    b) Notify the third-party application provider in writing
    c) Include specific reasons for the denial or discontinuation
    d) Provide, if applicable, steps the app developer can take to mitigate the risk and reapply for access

4. Discontinuation of Access
    a) Access shall be revoked immediately or within a defined timeframe based on the severity of the risk.
    b) The API key or token associated with the app shall be deactivated.
    c) Affected members shall be notified if required under HIPAA breach notification rules.

5. Appeals and Reinstatement

a) The third-party app provider may submit a written appeal with evidence of remediation.

b) The BHP shall re-evaluate the risk and determine whether access can be reinstated.

C. Compliance, Monitoring, and Change Management

1. This policy shall be reviewed annually or upon significant changes to federal regulations, technical changes, interoperability standards, or internal systems.

2. HCA change management procedures shall be used to plan and execute changes to the API as needed.

3. All actions taken under this policy shall be logged and retained for audit purposes.

III. Data Availability via Oracle Health's FHIR/API

A. The Health Care Agency has implemented Oracle Health's FHIR/API solution for patient Access API. Oracle Health's FHIR API supports timely access to patient data through a combination of infrastructure, standards compliance, and integration with national health information networks. Several factors contribute to near real-time or same-day data availability:

1. Key Factors Enabling Timely Data Access

a) FHIR Standard Implementation: Oracle Health uses HL7 FHIR (Fast Healthcare Interoperability Resources) R4 APIs, which are

designed for real-time data exchange. These APIs allow authorized users to access patient data directly from the Oracle Health Millennium Platform or Clinical Data Exchange systems.

b) Oracle Health Information Network: This network provides unified health data connectivity across Oracle Health customers. It includes intelligent patient matching and record location capabilities, which help ensure that the right data is retrieved quickly and securely

c) Integration with National Networks: Oracle Health is connected to national interoperability frameworks including CommonWell Health Alliance, which is a designated Qualified Health Information Network (QHIN) under the Trusted Exchange Framework and Common Agreement (TEFCA). This allows Oracle to exchange data with other EHRs and health systems across the country.

IV. Ensuring API Reliability and Regulatory Alignment

1. Testing of the Patient Access API shall be done on a quarterly basis and as needed with Regulatory changes, system upgrades, security audits and performance degradation.

2. HCA shall monitor changes related to the Interoperability and Patient Access Final Rule and ensure that the system continues to comply with the standards. In addition, HCA shall regularly test and validate APIs for functionality, security, and performance, monitor API usages, respond to issues or outages and stay updated with CMS guidance and enforcement updates.