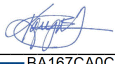
 <p><b>Behavioral Health Department</b> Alameda County Health</p>	<p>DocuSigned by:    By: _____  BA167CA0C0D444A...  <b>Karyn L. Tribble, PsyD, LCSW, Director</b></p>
<p><b>POLICY TITLE</b></p> <p>Interoperability and Patient Access</p>	<p><b>Policy No:</b> 300-5-1  <b>Date of Original Approval:</b> 5/10/2024  <b>Date(s) of Revision(s):</b></p>

**PURPOSE:**

To provide a policy regarding the requirement for Behavioral Health Plans (BHPs) to implement and maintain secure, standards-based Patient Access and Provider Directory Application Programming Interfaces (APIs), in compliance with the Centers for Medicare and Medicaid Services (CMS) Interoperability and Patient Access Final Rule and Department of Health Care Services (DHCS) issued [BHIN 22-068](#).

**BACKGROUND:**

In May 2020, CMS finalized the Interoperability and Patient Access Final Rule (CMS Interoperability Rule), which seeks to establish beneficiaries as the owners of their health information with the right to direct its transmission to third-party applications. CMS and the Office of the National Coordinator for Health Information Technology have established a series of data exchange standards that govern such specific transactions.

**SCOPE:**

This policy applies to all Behavioral Health Plans (BHPs), which includes Mental Health Plans (MHPs) and Drug-Medi-Cal Organized Delivery Systems (DMC-ODSs). The requirement includes information maintained by the BHP, in the BHP’s Electronic Health Record for County-owned and operated providers and/or information supplied to the BHP from sub-contracted providers.

**POLICY:**

BHPs shall implement and maintain a secure, standards-based Patient Access Application Programming Interface (API) and a publicly accessible, standards-based Provider Directory API

that can connect to mobile applications and be available through a public-facing digital endpoint on each BHP’s website. BHPs must also comply with 42 Code of Federal Regulations (CFR) 438.242, 45 CFR 170.215, the provider directory information requirements specified in 42 CFR 438.10, and the public reporting and information blocking components of the CMS Interoperability Rule 45 CFR Part 171.

BHPs must make individual-level United States Core Data for Interoperability (USCDI)<sup>1</sup> data that they maintain for dates of services on, or after, January 1, 2016, available to the beneficiary or their authorized representative as follows:

<b>Type of Information</b>	<b>Time by Which Information Must be Accessible</b>
Adjudicated claims data, including claim data for payment decisions that may be appealed, were appealed, or in the process of appeal, provider remittances, and beneficiary cost-sharing pertaining to such claims.	Within one (1) business day after a claim is processed.
Clinical data, including diagnoses and related codes and laboratory test results	Within one (1) business day after receiving data from providers.
Information about covered outpatient drugs and updates to such information, including formulary of prescription drugs, costs to the beneficiary and preferred drug list information, if applicable.	Within one (1) business day after the effective date of any such information or updates to such information.
Encounter data from providers compensated on the basis of risk-based capitation payments, as defined in 42 CFR 438.2.	Within one (1) business day after receiving data from providers.

**I. Description of the process used by the BHP for determinations to deny or discontinue any third-party application’s connection to an API.**

BHPs may deny or discontinue any third-party application’s connection to an API if it does not meet policies defined in [BHIN-22-068-Interoperability-and-Patient-Access-Final-Rule.pdf](#).

<sup>1</sup> [45 CFR § 170.213 - United States Core Data for Interoperability. | Electronic Code of Federal Regulations \(e-CFR\) | US Law | LII / Legal Information Institute \(cornell.edu\)](#)

## **II. Digital access to Designated Record Sets and Provider Directory**

Members are provided with detailed information regarding their right to access their records and ACBHD Provider Directory digitally. Instructions for digital access to Designated Record Sets and the Provider Directory will be posted on the [ACBHD Public website](#).

Members and their legal representatives have a right to access PHI in a Designated Record Set. A Designated Record Set is defined in 45 CFR 164.501 as a group of records maintained by, or for, a covered entity that comprises the:

- Medical records and billing records about individuals maintained by or for a covered health care provider;
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals. This last category includes records that are used to make decisions about any individuals, whether or not the records have been used to make a decision about the particular individual requesting access.

Members are encouraged to protect the privacy and security of their health information and understand the security and privacy practices of any application to which they entrust their health information. Educational information related to protection of PHI will be posted on the [ACBHD Public website](#).

## **III. Process to ensure data maintained by the BHP is available within one business day of receipt or within one business day after a claim is adjudicated or encounter data is received for dates of service on or after January 1, 2016.**

Members are able to register for digital access to their medical records at any time through a third-party application (e.g. Apple Health). Once registration has been completed, all non-redacted records are made available immediately without delay for any dates of service on or after January 1, 2016.

In order to comply with timeliness of data availability, data is synced between all systems (claims, demographics, encounters) at least once daily. Any errors or issues with synchronization are reported to administrative personnel for immediate review and remediation.

A Health Plan may deny access to records in certain circumstances as defined by Federal regulations.<sup>2</sup> The County-operated EHR will be designed to allow providers to restrict notes from viewing based on these regulations. Members have the right to request a review of the denial reason in certain circumstances. Information regarding these rights are posted on the [ACBHD Public website](#).

#### **IV. Process for ensuring that the Provider Directory API is updated no later than 30 calendar days after the BHP receives new information or is notified of any information that affects the content or accuracy of the provider directory**

To ensure compliance with timeliness (30 days) of data availability, data is synced between the county source of truth at least once weekly. Any errors or issues with synchronization are reported to administrative personnel for immediate review and remediation.

#### **V. Process for conducting routine testing and monitoring of the Patient Access and Provider Directory APIs, and system updates as appropriate to ensure the APIs are compliant with the technical, privacy, and security functions outlined in the Interoperability and Patient Access Final Rule.**

A weekly report including summary data for API access, requests, and authentication failures will be generated and sent to administrative personnel. Additionally, the Patient Access and Provider Directory APIs log requests, authorization attempts, unauthorized requests, and malformed requests are available to administrative personnel upon request.

Automated API testing is performed monthly using a program and a set of evolving parameters designed to capture common requests and results. The parameters are adjusted periodically to reflect general API functionality, as well as specific searches or issues which have been identified through audit information during normal use.

#### **VI. Utilization Metrics for Patient Access API and Provider Directory API**

The following Patient Access API utilization metrics will be captured on a quarterly basis by ACBHD for the County's Electronic Health Record:

- Total API pass and error rates
- Count of Unique API Consumers making API requests
- Count of Third-party Applications registered with the API

---

<sup>2</sup> [45 CFR § 164.524 - Access of individuals to protected health information. | Electronic Code of Federal Regulations \(e-CFR\) | US Law | LII / Legal Information Institute \(cornell.edu\), CFR-2011-title45-vol1-sec164-524.pdf \(govinfo.gov\)](#)

The following Provider Directory API utilization metrics will be captured by ACBHD and shared with DHCS on a quarterly basis:

- Total API pass and error rates
- Count of unique Third-Party Applications making API requests

**NON-COMPLIANCE**

Per Section 1 of this policy, ACBHD may deny or discontinue any third-party application’s connection to an API if it does not meet policies defined in [BHIN-22-068-Interoperability-and-Patient-Access-Final-Rule.pdf](#).

**CONTACT**

ACBHD Office	Current Date	Email/Phone
API Policy	5/9/2024	<a href="mailto:API-Policy@acgov.org">API-Policy@acgov.org</a>

**DISTRIBUTION**

This policy will be distributed to the following:

- ACBHD Staff
- ACBHD Contract Providers
- Public

**ISSUANCE AND REVISION HISTORY**

**Original Authors:** Sudesh Gadewar, Security Officer, ACG

**Original Date of Approval:** 5/10/2024

Revision Author	Reason for Revision	Date of Approval by (Name, Title)

## Definitions

<b>Confidentiality</b>	Under the Security Rule, confidential ePHI is that ePHI that may not be made available or disclosed to unauthorized persons.
<b>Integrity</b>	Under the Security Rule, to maintain the integrity of ePHI means to not alter or destroy it in an unauthorized manner.
<b>Availability</b>	Under the Security Rule, PHI is considered to be “available” when it is accessible and usable on demand by an authorized person.
<b>Public-facing digital endpoint</b>	A Digital endpoint is a digital location where a Digital end point receives requests about a specific resource on its server. In APIs, an endpoint is typically a uniform resource locator (URL) that provides the location of a resource on the server