SAN BERNARDINO COUNTY | Behavioral Health

303 E. Vanderbilt Way San Bernardino | (909) 388-0900
***www.SBCounty.gov***

# Client API Access, Control, and Availability Policy

DocuSigned by:
Dr. Georgina Yoshioka
7DF8077EFA674B2...

| | | |
|---|---|---|
| **Effective Date** | 05/08/2025 | |
| **Revised Date** | 05/08/2025 | Georgina Yoshioka, DSW, MBA, LCSW, Director |

**Policy**

It is the policy of the Department of Behavioral Health (DBH) to ensure that DBH clients can access their electronic health record (EHR) via the Patient Access API in accordance with the CMS Interoperability and Patient Access Final Rule (BHIN 22-068 and BHIN 22-032).

**Purpose**

To provide instruction for making client records and billing information accessible to the client and to inform DBH staff of guidelines regarding the Application Programming Interface (API) and Third-Party Vetting Application process.

**Definitions**

**Application Programming Interface (API)**: A set of rules and protocols that allow different software applications to communicate with each other.

**Deprovisioning**: The process of removing user access to software and network services.

**Encryption**: The process of converting information or data into a code to prevent unauthorized access:

**Explanation of Benefits (EOB**): A written statement that describes the costs involved for visits to a provider and what costs insurance will cover.

**Provisioning**: The process of making information technology (IT) systems available to users

**Risk Analysis**: A systematic process used to identify potential hazards and evaluate the associated risks within a specific context.

**Transport Layer Security**: a security protocol designed to facilitate privacy and data security for communications over the Internet.

**Healthcare Claims Information**

Client healthcare claims and payment information is sent as an electronic submission from healthcare providers to health insurance companies (payors). These claims may be referred to as an “835 file”. San Bernardino Mental Health Plan and Substance Use Disorder Treatment Plan submit claims to Medi-Cal and other insurance providers for the services provided to clients through myAvatar Cal-Practice Management (Cal-PM).

*Continued on next page*

**Healthcare Claims Information,** continued

- The following information should be included in all claims:
  - What charges were paid/reduced/denied.
  - Deductible/co-insurance/co-pay amounts, and
  - Bundling and splitting of claims, and how the payment was made.
- Only data electronically received and posted via a claim will be listed in the Explanation of Benefits (EOB) resource and available for electronic viewing;
- In myAvatar Cal-PM, data will be available once the claim / 835 file has been posted in the "835 health Claim Payment/Advice" form, and
- Once a Medi-Cal claim is submitted for processing and payment, this data will be available.

**Data Availability for Client Access**

Clients have the right to access their own medical records. Client records and billing information (see above section) will be updated within the following timelines:

| **Data Type** | **Timeframe** |
|---|---|
| Adjudicated claims, including claims data for payment decisions that may be appealed, were appealed, or are in the process of appeal, provider remittances and client cost-sharing pertaining to such claims. | Within one (1) business day after a claim is processed |
| Encounter data | No later than one (1) business day after receiving the data from providers, other than MCOs, PHIPs, and PAHPs, compensated on the bases of capitations payment. |
| 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 or prescription drugs, costs to the client, 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. |

**Note:** Clients may obtain their medical records produced after January 1, 2016, and prior to the establishment of the electronic health record, by submitting form COM021 Access to Medical Records form to DBH-MedicalRecords@dbh.sbcounty.gov or by contacting the Medical Records Unit at (909) 421-9350.

*Continued on next page*

**Third-Party Application Vetting**

In response to CMS Interoperability and Patient Access Final Rule, DBH established the Patient Access API which promotes the employment of provisioning decisions to ensure a system is created that allows client data to be managed and accessed effortlessly. Provisioning decisions will be informed by the following:

- Provision Decisions conducted by IT:
  - Compliance with CMS Interoperability specification, including adherence to data exchange standard and protocols ensuring seamless data interoperability.
  - Acceptable security criteria, such as encryption standards, data integrity measures, and regular security audits.
  - Encryption Standards
    - Data in Transit: Use Transport Layer Security (TLS) 1.2 or higher for all communications between the client and server. This ensures that data transmitted over the internet is securely encrypted.
    - Data at Rest: Encrypt sensitive data stored on servers using strong encryption standards such as AES (Advanced Encryption Standard) 256-bit encryption. This protects the data from unauthorized access if the physical security of the storage medium is compromised.
    - Data Integrity Measures: Adhere to HIPAA Security Rule integrity standards. This ensures the client's ePHI is not altered or destroyed in an unauthorized manner.
    - Digital Signatures: Implement digital signatures to ensure data integrity and non-repudiation. This involves using cryptographic algorithms to generate a digital signature based on the data, which can then be verified by the recipient to ensure that the data has not been altered in transit.
    - Audit Logging: Maintain comprehensive and tamper-evident audit logs that record log access and actions performed on health data. This helps in monitoring and investigating unauthorized access or modifications.
  - Evidence of Regular Security Audits
    - Internal Audits: Conduct regular internal security audits to assess the effectiveness of security measures in place. This can involve reviewing security policies, access controls, encryption practices, and audit logs.
    - External Audits and Certifications: Engage third-party security firms to conduct external audits and obtain certifications such as HITRUST CSG or ISO/IEC 27001. These audits provide an independent assessment of the organization's compliance with recognized security standards.

*Continued on next page*

**Third-Party Application Vetting,** continued

        - Penetration Testing: Perform regular penetration testing to identify and address vulnerabilities in the API and the underlying infrastructure. This involves simulating cyber-attacks under controlled conditions to evaluate the system's resilience to such threats.
    - Ongoing Compliance with Regulations:
        - Ensure compliance of relevant healthcare data protection guidelines are in accordance with state, federal, and local laws and/or regulations (i.e. Health Insurance Portability and Accountability Act). These regulations often specify minimum security requirements that must be met.

**Denial or Discontinuation of Third-Party Access**

In accordance with DHCS Behavioral Health Information Notice NO: 23-032, criteria for Third-Party access denial are as follows:

- Decision-Making Process
    - Evidence of non-compliance with HIPAA and CMS Interoperability standards.
    - Outcomes of security risk assessments and incident reports.
    - County inclusion in the decision-making process, ensuring that any third-party app decisions are made with county oversight and in consultation with relevant stakeholders.
    - If DBH reasonably determines that a third-party application presents unacceptable level of risk to PHI, the decision to deny or discontinue the applications' connection to the DBH API will be made by the Security Officer in consultation with the Compliance Officer and IT Leadership.
    - The third-party application provider will be notified in writing of the decision to deny or discontinue access, including the specific reasons for the decision and, if applicable, steps that could be taken to mitigate the identified risks.
- DBH may deny or discontinue any third-party application's connection to the API if DBH:
    - Reasonably determines, consistent with its security risk analysis under 45 CFR part 164 subpart C, that allowing an application to connect or remain connected to the API would present an unacceptable level of risk to the security of protected health information on the State's systems; and
    - Makes this determination using objective, verifiable criteria that are applied fairly and consistently across all apps and developers through which parties seek to access electronic health information, as defined in 45 CFR 171.102, including but not limited to criteria that rely on automated monitoring and risk mitigation tools.

*Continued on next page*

**Documentation and Record Keeping of Third-Party Access Denials**

All decisions to approve, deny or discontinue access along with the rationale and any correspondence with the third-party application provider, will be thoroughly documented and retained in accordance with Health Services Agency standards. Documentation and record keeping of specific documents are as follows:

- Application Vetting Documents
  - Security and Compliance Assessments: Documentation of the third-party applications compliance with CMS Interoperability specifications, HIPAA, and any other relevant regulations. This should include detailed assessments of their adherence to encryption standards for data in transit and at rest, data integrity measures, and digital signatures.
  - Audit Reports: Copies of recent internal and external security audits reports, including penetration testing results and certifications like HITRUST CSF or ISO/IEC 27001.
  - Regulatory Compliance Evidence: Proof of ongoing compliance with healthcare data protection regulations (e.g., HIPAA, GDPR) through policy documents, training records, or compliance certificates.
- Risk Analysis Documentation
  - Risk Assessment Reports: Detailed reports from the risk analysis process highlighting potential risks associated with granting access to the third-party application, including:
    - Assessments of non-compliance with HIPAA;
    - History of data breaches;
    - Encryption standards, and
    - The timeliness of security updates.
- Decision Documentation
  - Decision Making Records: Documentation outlining the decision process for granting, denying, or discontinuing access. This should include:
    - Minutes from meetings;
    - Email correspondences, and
    - Written statements from the Security Officer, Compliance Officer, and IT leadership detailing their reasoning and the evidence considered.
  - Notification Letters: Copies of written notifications sent to third-party application providers regarding the decision to grant, deny, or discontinue access, including reasons and potential steps for mitigation.
- Appeal Process Documentation
  - Appeal Requests and Responses: Documentation related to any appeals submitted by third-party providers, including their initial appeal letter, any additional information or corrective measures they provide, and the final decision from DBH.

*Continued on next page*

**Documentation and Record Keeping of Third-Party Access Denials,** continued

- Monitoring and Review Documents
  - Continuous Monitoring Reports: Ongoing reports and logs that track the third-party applicant's compliance with agreed-upon security and privacy standards.
  - Security Risk Analysis Updates: Periodic updates from security risk analyses conducted post-approval to identify any new risks;
  - Provisioning and Deprovisioning Records;
  - Report Forms: Completed forms or support cases submitted for access changes, including details such as
    - The desired date for enablement/disablement;
    - Environments for access, and
    - The third-party applications use case;
  - Change Logs: Logs or records documenting any changes to the access of third-party applications over time.
- Policies and Procedures: A comprehensive manual or documentation set that includes all policies and procedures related to third-party application access to the FHIR API, including this documentation policy.

**Regular Security Risk**

The Security Risk Analyses to be completed by IT are as follows:

- Regular Security Risk Analysis:
  - Consistent with the HIPAA Security Rule, and
  - Conduct regular and ad-hoc security risk analyses to identify potential risks to PHI within DBH systems, including those that may arise from third-party application access.
- Criteria for Unacceptable Risk:
  - Factors considered in determining an unacceptable level of risk include, but are not limited to:
    - Non-compliance with HIPAA;
    - Evidence of data breaches or security incidents;
    - Inadequate encryption standards, and
    - Lack of timely security updates.

**Referenced Forms, Policies, and Procedures**

DBH Standard Practice Manual and Departmental Forms:

- Client API Access, Control, and Availability Procedure (IT5026-1)
- Provider Directory Policy (IT5027)
- Access To Medical Records Request (COM021)
- Release Of Information: Patient's Right Of Access To His/her Own Medical Record (COM026)
- Access And Amendment Of Medical Records Policy (COM0931)

*Continued on next page*

**Referenced Forms, Policies, and Procedures,** continued

Developer API Resources – DBH Internet Website

- Developer Access Request Form – DBH Internet Website

**Reference(s)**

- Assembly Bill (AB) 133
- BHIN 22-032 Interoperability and Patient Access Final Rule Compliance Monitoring Process
- BHIN 22-068 Interoperability and Patient Access Final Rule
- CMS Interoperability Rule & CMS Interoperability Specification
- Cures Act
- Health and Safety Code section 130290
- Welfare and Institutions Code (W&I) section 14184.100, et seq.