SAN BERNARDINO COUNTY
Behavioral Health
303 E. Vanderbilt Way San Bernardino | (909) 388-0900
www.SBCounty.gov

INTERIM INSTRUCTION NOTICE #24-002

October 1, 2024

SUBJECT: Application Programming Interface (API) Access Control & Third-Party Application Management for MHP & DMC-ODS

DISTRIBUTION: **Department of Behavioral Health procedure**

OBSOLETE: **Upon completion of related policy and/or**

Effective Date October 1, 2024

From Department of Behavioral Health (DBH) Information Technology (IT)

Introduction

The purpose of this Interim Instruction Notice (IIN) is to inform Department of Behavioral Health (DBH) staff of guidelines regarding the Application Programming Interface (API) and Third-Party Vetting Application process. These new processes aim to enhance access to care and guarantee that clients possess the necessary information to make well-informed decisions concerning their healthcare.

Background

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

Assembly Bill (AB) 133 (Committee on Budget, Chapter 143, Statutes of 2021) implements various components of the CalAIM initiative, including those components in Welfare and Institutions Code (W&I) section 14184.100, et seq., and Health and Safety Code section 130290 to implement the California Health and Human Services Data Exchange Framework, including the CMS Interoperability Rule. The Department of Health Care Services is authorized to develop and implement Article 5.51 of the W&I Code and the requirements of the California Health and Human Services Data Exchange Framework. This San Bernardino County Department of Behavioral Health interim instruction notice (IIN) supports this implementation.

Continued on next page

Scope

This IIN applies to all System Administrators, IT Managers, IT staff, security personnel, and any other employees involved in overseeing and/or managing third-party application access to San Bernardino County Department of Behavioral Health APIs. It also extends to all third-party applications that are able to view access to these APIs.

Third-Party Application Vetting

In response to CMS Interoperability and Patient Access Final Rule, API emerged promoting the establishment 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:

a) Provision Decisions conducted by IT:
    i. Compliance with CSM Interoperability specification, including adherence to data exchange standard and protocols ensuring seamless data interoperability.
    ii. Acceptable security criteria, such as encryption standards, data integrity measures, and regular security audits.
    iii. Encryption Standards
        a. 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.
        b. 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.
        c. 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.
        d. 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.
        e. 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.
    iv. Evidence of Regular Security Audits
        a. 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.

Continued on next page

Third-Party Application Vetting, continued

b. 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.
c. 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.

v. Ongoing Compliance with Regulations:
a. 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.

Provisioning and Deprovisioning Process

The provision and deprovision process is triggered by the submission of an API Development Access Request form from a third-party developer requesting access to the San Bernardino County API. The request form is currently under development but will be posted on the Department of Behavioral Health webpage once finalized.

After completing the review outlined in section (a) of the Third-Party Application Vetting block (notated on page 2), IT support will proceed with the following:

a) Open a support case via the NetsmartConnect Support Portal
b) Include the following details in the support case:
   i. Desired date for access enablement or disablement.
   ii. Environments to which access is to be granted or removed (e.g., production, testing).
   iii. Name of third-party application.
   iv. Use case of the third-party application.
c) Once the Third-Party is approved and Netsmart has processed the support ticket, the Third-Party Applicant will then follow the process that will be indicated on the San Bernardino County Department of Behavioral Health Provider Directory and Patient Access Application Program Interfaces (APIs) webpage. This webpage is currently under development.

Continued on next page

Denial or Discontinuation of Access

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

a) Decision-Making Process
   i. Evidence of non-compliance with HIPAA and CMS Interoperability standards.
   ii. Outcomes of security risk assessments and incident reports.
   iii. 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.
   iv. If San Bernardino Conty Department of Behavioral Health 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.
   v. 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.

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, San Bernardino County Department of Behavioral Health will conduct regular, and ad-hoc security risk analyses to identify potential risks to PHI, within out 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.

Documentation Records

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:

a) Application Vetting Documents
   i. 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.

Continue on next page

Documentation Records, continued

ii. Audit Reports: Copies of recent internal and external security audits reports, including penetration testing results and certifications like HITRUST CSF or ISO/IEC 27001.
iii. Regulatory Compliance Evidence: Proof of ongoing compliance with healthcare data protection regulations (e.g., HIPAA, GDPR) through policy documents, training records, or compliance certificates.

b) Risk Analysis Documentation
   i. 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.

c) Decision Documentation
   i. 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 Office, Compliance Officer, and IT leadership detailing their reasoning and the evidence considered.
   ii. 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.

d) Appeal Process Documentation
   i. 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 San Bernardino County Department of Behavioral Health.

e) Monitoring and Review Documents
   i. Continuous Monitoring Reports: Ongoing reports and logs that track the third-party applicant's compliance with agreed-upon security and privacy standards.
   ii. Security Risk Analysis Updates: Periodic updates from security risk analyses conducted post-approval to identify any new risks.

Continued on next page

iii. Provisioning and Deprovisioning Records
iv. 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.
v. Change Logs: Logs or records documenting any changes to the access of third-party applications over time.

f) Policies and Procedures: A comprehensive manual or documentation set that includes all policies and procedures related to the third-party application access to the FHIR API, including this documentation policy.

Client /Patient API Access

Client/Patient API access is as follows:

a) CBH Client: The third-party should ask the client to link their data from their health plan. They should follow the instructions on their App to start the linking process.
b) Client Log In: The client will need to log into their San Bernardino County Department of Behavioral Health account. The App will direct client to the San Bernardino County Department of Behavioral Health Log In screen. If client has set up a myHealthPointe member account with the San Bernardino County Department of Behavioral Health, they will enter a Username and Password. If they have not yet set up their San Bernardino County Department of Behavioral Health account, they will need to set up their account from this screen.
    i. Client will will click on the Register Now link from the Log In screen.
    ii. They will need to type in their name, date of birth, zip code, Enrollee ID, and either their email address or cell phone number.
    iii. Create a username and password. When they do this, a 6-digit code will be sent to them, they will get either an email or a text to their cell phone. Client enters this code on the registration page to complete the account setup process.
    iv. Before the 6-digit code is sent to the client IT must search for the client and send the patient an authorization token via myAvatar.
c) Complete the Form: The client will receive an email with the link and will be sent to a page that will request they fill in their name, home address, San Bernardino County Department of Behavioral Health Enrollee ID and phone number. Client should look at all the information that can be shared. If there is information client does not want to share, they will need to uncheck the box next to that information. When they click Submit, their data will be shared with the App.

Continued on next page

Client /Patient API Access, continued

d) Patient Support: Should the patient encounter any issues accessing their data within their App, they should seek support through their vendor APP initially. Should the problem extend beyond the scope of the vendor's application, the vendor will follow the Support Protocol notated below.

Support Protocol

Troubleshooting Steps for Third-Part Application Vendor

a) Initial Assessment: Vendors should first conduct an internal review to identify the issue's nature and scope
b) Consult Documentation: Review Netsmart's API documentation and FAQs for potential solutions or similar issues.
c) Contact Support: If unresolved, the vendor should contact the Department of Behavioral Health's IT via a specified support channel, providing:
    i. A detailed description of the issue.
    ii. Relevant error messages or codes.
    iii. Impact assessment on users.
    iv. Steps already taken to attempt resolution.
d) Collaboration for Resolution: Work collaboratively with the Department of Behavioral Health's IT to diagnose and resolve the issue, keeping detailed records of the interaction and solutions provided.

Reference(s)

- CMS Interoperability Rule & CMS Interoperability Specification
- Assembly Bill (AB) 133
- Welfare and Institutions Code (W&I) section 14184.100, et seq.
- Health and Safety Code section 130290
- Cures Act

Questions

For questions regarding this Interim Instruction Notice, please contact DBH IT at (909) 386-9730 or via email at dbh-it-helpdesk@dbh.sbcounty.gov.