SANTA CRUZ COUNTY
Behavioral Health Services

POLICIES AND PROCEDURE MANUAL

Subject: Application Programming Interface (API) Access Control & Third-Party Application Management for MHP & DMC-ODS	**Policy Number: 4305** **Reference to BHIN No. 22-068**
Date Effective: 3/1/2024	**Pages: 7**
Replaces: N/A	**Responsible for Updating: Information Technology (IT) & BH Administration**
Approval: DocuSigned by: Jiffany Cantrell-Warren 89088AF6B9B64AE... Behavioral Health Director	2/29/2024 Date

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.[1][2] 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.[3]

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.[4] This Santa Cruz County Behavioral Health policy supports this implementation.

SCOPE:

This policy is applicable to System Administrators, IT Managers and IT staff, security personnel, and any other employees involved in overseeing or managing third-party application access to Santa Cruz County Behavioral Health's APIs. It also extends to all third-party applications that seek access to these APIs.

---

[1] 85 Federal Register 25510-25640.
[2] Section 4003 of the Office of the National Coordinator for Health Information Technology 21st Century Cures Act defines "Interoperability" as health information technology that (1) enables the secure exchange and use of electronic health information without special effort on the part of the user; (2) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law; and (3) does not constitute information blocking as defined in section 3022(a) of the Public Health Service Act.
[3] The data exchange standards for the Patient Access Application Programming Interface; CARIN Implementation Guide; Payer Data Exchange for US Drug Formulary; Provider Directory Application Programming Interface.
[4] W&I section 14184.102(d); HSC section 130290(j).

PURPOSE:

Provider Directory API: The Provider Directory Application Program Interface (API) is a recent development aimed at delivering current details regarding healthcare providers and facilities to beneficiaries of the Centers for Medicare & Medicaid Services (CMS). Through this API, beneficiaries can explore healthcare providers and facilities based on various factors such as location, specialty, and other criteria.

This API emerged as a response to the CMS Interoperability and Patient Access Final Rule. This regulation mandates health plans to furnish beneficiaries with access to precise and promptly updated provider directory information through an API. The rule's objective is to enhance access to care and guarantee that beneficiaries possess the necessary information to make well-informed decisions concerning their healthcare.

DEFINITIONS:

1. **Patient:** An individual who is receiving or has received health care services.
2. **CMS Interoperability:** The set of regulations and technical standards established by the Centers for Medicare & Medicaid Services to ensure health information technology systems can exchange and make use of information without special effort on the part of the user.
3. **Patient Access API:** An interface developed and hosted by Netsmart, designed to provide up-to-date information about healthcare providers and facilities to patients and healthcare consumers.
4. **Interoperability:** The ability of different information systems, devices, or applications to access, exchange, integrate, and cooperatively use data in a coordinated manner, within and across organizational boundaries.
5. **Protected Health Information (PHI):** Information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can link to a specific individual.

POLICY:

1. Third-Party Application Vetting

a) Provisioning Decisions: Decisions will be informed by:

i. Compliance with CMS Interoperability specifications, including adherence to data exchange standards 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 TLS (Transport Layer Security) 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

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 access to 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 the security measures in place. This can involve reviewing security policies, access controls, encryption practices, and audit logs.
b. External Audits and Certifications: Engage third-party security firms to conduct external audits and obtain certifications such as HITRUST CSF 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 with relevant healthcare data protection regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the United States, GDPR (General Data Protection Regulation) in the European Union, or other local regulations. These regulations often specify minimum security requirements that must be met.

2. Risk Analysis

a) Criteria for Unacceptable Risk: Non-compliance with HIPAA, history of data breaches, inadequate encryption, and delayed security updates are considered unacceptable risks.

3. Denial or Discontinuation of Access

a) Decision Process: In line with DHCS Behavioral Health Information Notice No: 23-032, criteria for decision-making include:

i. Evidence of compliance or non-compliance with HIPAA and CMS Interoperability standards.
ii. 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 Santa Cruz County Health Services Agency reasonably determines that a third-party application presents an unacceptable level of risk to PHI, the decision to deny or discontinue the application's connection to our 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.

b) **Appeal process**: The third-party application provider will have the opportunity to respond to the decision, provide additional information, or detail corrective measures taken to address the concerns raised by Santa Cruz County Health Services Agency.
c) **Continuous Monitoring**: Once access is granted, Santa Cruz County Health Services Agency will continuously monitor the third-party application's adherence to agreed-upon security and privacy standards.

4. Regular Security

a) Regular Security Risk Analysis: Consistent with the HIPAA Security Rule, Santa Cruz County Health Services Agency will conduct regular, and ad-hoc security risk analyses every 30 days to identify potential risks to PHI within our systems, including those that may arise from third-party application access.

d) 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.

5. Documentation and Record Keeping: All decisions to 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.

PROCEDURES:

1. **Provisioning and Deprovisioning Process**
   The process is triggered by the submission of a request form. The Third Party Developer submits requests access via a form available on our public facing web site www.santacruzhealth.org: After completing the review outlined in section 1(a) of this policy IT support will
   i) Open a support case via the NetsmartCONNECT Support Portal
   ii) Include the following details in the support case:
      (1) Desired date for access enablement or disablement.
      (2) Environments to which access is to be granted or removed (e.g., production, testing).
      (3) Name of the third-party application.
      (4) Use case of the third-party application.
   iii) Once the Third Pary is approved and Netsmart has processed the support ticket the third party will then follow the process as it is laid out on our externally facing

web site under on the Santa Cruz County Behavioral Health Services Provider Directory and Patient Access Application Program Interfaces (APIs) page

2. Documentation

(1) Application Vetting Documents
- (a) Security and Compliance Assessments: Documentation of the third-party application's 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.
- (b) Audit Reports: Copies of recent internal and external security audit reports, including penetration testing results and certifications like HITRUST CSF or ISO/IEC 27001.
- (c) Regulatory Compliance Evidence: Proof of ongoing compliance with healthcare data protection regulations (e.g., HIPAA, GDPR) through policy documents, training records, or compliance certificates.

(2) Risk Analysis Documentation
- (a) 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.

(3) Decision Documentation
- (a) 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.
- (b) 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.

(4) Appeal Process Documentation
- (a) 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 Santa Cruz County Health Services Agency.

(5) Monitoring and Review Documents
- (a) Continuous Monitoring Reports: Ongoing reports and logs that track the third-party application's compliance with agreed-upon security and privacy standards.
- (b) Regular Security Risk Analysis Updates: Periodic updates from security risk analyses conducted post-approval to identify any new risks.
- (c) Provisioning and Deprovisioning Records
- (d) Access Request Forms: Completed forms or support cases submitted for access changes, including details like the desired date for enablement/disablement, environments for access, and the third-party application's use case.
- (e) Change Logs: Logs or records documenting any changes to the access levels of third-party applications over time.

(6) Policies and Procedures

(a) Policies and Procedures Manual: 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.

3. **Client/Patient API Access**
   (1) **Our Patient / Client:** In their App it should ask them to link their data from their health plan. They should follow the instructions on their App to start the linking process.
   (2) **Patient Log In:** The patient will need to log into their Santa Cruz County Behavioral Health Account. Their App will send you to the Santa Cruz County Behavioral Health Log In screen. If they have set up a myHealthPointe member account with Santa Cruz County Behavioral Health, they will enter a Username and Password. If they have not yet set up your Santa Cruz County Behavioral Health account, they will need to set up your Santa Cruz County Behavioral Health account from this screen.
   Follow these simple steps:
   (a) They will click on the Register Now link from the Log In screen.
   (b) They will need to type in their name, date of birth, zip code, Enrollee ID, and either their email address or cell phone number.
   (c) Create a username and password. When they do this, a 6-digit code will be sent to them. You will get either an email or a text to your cell phone. Enter this code on the registration page to complete the account setup process.
   (d) Before the 6-digit code is sent to the Patient/Client BH IT must search for the client and then send the patient an authorization token via myAvatar.
   (3) **Complete the Form.**
   The patient/client will receive an email with a link on it and they will be sent to a page that will request they fill in their name, home address, Santa Cruz County Behavioral Health Enrollee ID and phone number. They should look at all the information that can be shared. If there is information they do 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.
   (4) **Patient Support**
   (a) Should the patient encounter any issues accessing 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 Section 4. Support Protocol.

4. Support Protocol
Troubleshooting Steps for Third-Party Application Vendors
   (1) **Initial Assessment**: Vendors should first conduct an internal review to identify the issue's nature and scope.
   (2) **Consult Documentation:** Review Netsmart's API documentation and FAQs for potential solutions or similar issues.
   (3) **Contact Support:** If unresolved, the vendor should contact BH IT via the specified support channel, providing:
   (a) A detailed description of the issue.
   (b) Relevant error messages or codes.

(c) Impact assessment on users.
(d) Steps already taken to attempt resolution.

(4) **Collaboration for Resolution:** Work collaboratively with BH IT to diagnose and resolve the issue, keeping detailed records of the interaction and solutions provided.

PRIOR VERSIONS: N/A

REFERENCES: CMS Interoperability Rule & CMS Interoperability Specifications, Assembly Bill (AB) 133, Welfare and Institutions Code (W&I) section 14184.100, et seq., Health and Safety Code section 130290, Cures Act, CARIN Implementation Guide

FORMS/ATTACHMENTS: None