Los Angeles County | Department of Mental Health | Chief Information Office Bureau

API Educational Materials version 1.0

LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

Revision and Sign-off Sheet

Version History

Date	Author	Version	Change Reference
09/30/2024	LACDMH Integration Team	1.0	Initial Release

Reviewers

Name	Version Approved	Position	Date
William Griffin	202401	IT Manager	09/30/2024

Distribution

Name	Position
Trading Partners and their IT vendors	N/A

Document Properties

Item	Details
Document Title	API Educational Materials version 1.0
Author	LAC DMH Integration Team
Creation Date	September 30, 2024
Last Updated	September 30, 2024

Contents

Background:

In May 2020, the Centers for Medicare and Medicaid Services (CMS) finalized the Interoperability and Patient Access final rule (CMS Interoperability Rule), which gives you the right to see your own health data thus establishing beneficiaries (You) as the owners of your health information with the right to direct its transmission to third-party applications.

As healthcare providers, Los Angeles County Department of Mental Health (LACDMH) is obligated to protect your privacy. You may be asked to provide your data to others. Please note that they may not have the same strict obligations. LACDMH is required to provide you with access to detailed information about your health history through a "Patient Access API (application programming interface)." You may access this information by downloading a third party application (App) on your smart phone, tablet, computer or other similar device.

What are Third-Party-Applications?

Third-party applications are software programs or services that are not developed by Los Angeles County Department of Mental Health (LACDMH), bur developed by some other entities. These applications can leverage the data made available through Patient Access APIs to provide patients with additional functionalities or services.

Examples of third-party applications might include:

- Health apps: These apps can help patients track their health metrics, manage medications, or find nearby healthcare providers.
- Fitness trackers: These devices can integrate with Patient Access APIs to sync health data and provide more comprehensive insights.
- Financial management tools: These tools can help patients understand the costs of healthcare services and manage their health insurance plans.

Essentially, third-party applications serve as intermediaries that connect patients with their health data, enabling them to access and utilize their information in various ways beyond the traditional electronic health record (EHR). LACDMH provide your chosen Third-Party-Apps access to your health data. This is done through a Patient Access API (Application Programming Interface).

What is an API?

A simple way for two pieces of software to communicate with one another to get data. An example is when you send a message using a cell phone. LACDMH developed Patient Access API that allows you to communicate with LACDMH's electronic health record system using your Third-Party-App to retrieve Healthcare Data.

What is Healthcare Data?

Health data is information about your medical history, treatment for substance use disorders, mental health, HIV status, and/or other sensitive information. It could be demographic information and information about medical tests you have had, any medical conditions you might have had, and more. claims and encounter information including cost, specifically provider remittances and enrollee cost-sharing, as well as a defined sub-set of their clinical information through third-party applications of their choice.

Benefits of API Data Exchange for Patients

API data exchange between patients and their providers offers several advantages:

Improved Access to Health Information

- **Real-time access:** Patients can access their health records at any time, from anywhere.
- **Consolidated view:** All health information can be viewed in one place, making it easier to manage.

Enhanced Patient Engagement

- **Increased involvement:** Patients can be more actively involved in their care by having access to their health data.
- **Better decision-making:** Informed patients can make more informed decisions about their healthcare.

Improved Care Coordination

- **Streamlined communication:** Healthcare providers can easily share information with each other, leading to better coordination of care.
- **Reduced errors:** The risk of medical errors can be reduced by having accurate and up-to-date information.

Increased Efficiency

- **Reduced administrative burden:** The need for manual data entry can be reduced, saving time and resources.

- **Faster access to care:** Patients can get faster access to care by having their health information readily available.

Greater Privacy and Security

- **Improved control:** Patients have greater control over their health information.
- **Enhanced security:** API data exchange can be made more secure than traditional methods of sharing data.

Overall, API data exchange offers significant benefits to patients, including improved access to health information, enhanced patient engagement, better care coordination, increased efficiency, and greater privacy and security.

PRIVACY and SECURITY:

Patient Access API will allow LACDMH to share your health data with the third party App you'll choose. However, LACDMH has no control over how your App will use or share your health data.

So to protect privacy and security of healthcare data use the following guidelines:

What to look for when choosing a third-party App:

Your App will have access to all your heath data once you allow it. You should read your App's privacy policy to see how this App may use your data. Make sure that you are comfortable with their rules. An App that publishes a privacy notice must do what it says in that notice. In general do the following before making a final decision on choosing an App:

- Research and review: Look for applications that have a strong reputation for data security and privacy.
- Check for certifications: Look for certifications like HIPAA compliance, which indicates the application meets specific security standards.
- Read privacy policies: Carefully review the privacy policy to understand how the application collects, uses, and protects your data.

So before you choose a third-party-App, you might want to go through the following list of questions to make an informed decision:

- What health data will this app collect? Will this app collect non-health data from my device, such as my location?
- Will my data be stored in a de-identified or anonymized form?
- How will this app use my data? Will this app disclose my data to third parties?
- Will this app sell my data for any reason, such as advertising or research?
- Will this app share my data for any reason? If so, with whom? For what purpose?
- Will your App let you control how it can use your data?
- How can I limit this app's use and disclosure of my data?
- What security measures does this app use to protect my data?
- What impact could sharing my data with this app have on others, such as my family members?
- How can I access my data and correct inaccuracies in data retrieved by this app?
- Does this app have a process for collecting and responding to user complaints?
- If I no longer want to use this app, or if I no longer want this app to have access to my health information, how do I terminate the app's access to my data?
- What is the app's policy for deleting my data once I terminate access? Do I have to do more than just delete the app from my device?
- How does this app inform users of changes that could affect its privacy practices?

If the app's privacy policy does not clearly answer the above questions, you should reconsider using this app. Since Health data is very sensitive, choose an app with strong privacy and security standards to protect the data. For more information from the FTC, refer to: How To Protect Your Privacy on Apps

Apps and HIPPA:

HIPPA is the Health Insurance Portability and Accountability Act. This is a federal law that says your health information cannot be shared unless it is for health care treatment, payment or operations and other reasons allowed by the federal law. The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule. To learn more about your rights under HIPAA, visit HHS.gov

Most third-party apps will not be covered by HIPAA. Instead, they fall under the jurisdiction of the Federal Trade Commission (FTC) and the protections provided by the FTC Act. The FTC Act, among other things, protects against deceptive acts (e.g., if an app shares personal data without permission, despite having a privacy policy that says it will not do so). The FTC provides

information about mobile app privacy and security for consumers here: https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps

Sharing Health Data online safe?

When making decisions about your health, you should only share your health data with people and apps you trust. These includes your family or doctors or others you see or rely on for care. Never share your username or password. Only use software you trust and always use a password on your phone, tablet, or computer. Do not send any data by email unless you can protect it with a password. For more information regarding online security refer to: Federal Trade Commission (FTC) Online Security

Note: Minors who are under the age of 13 are not allowed to share their health data unless their parent, guardian, or other personal representative gives approval.

Tips to keep information safe:

Here are a few tips:

- Only use trusted health apps.
- Keep your passwords and log-in information private.
- Keep your private papers in a secure place.
- Purchase virus protection software for your computer.

HIPAA-Covered Entities: A Breakdown

Certain organizations and individuals are considered HIPAA-covered entities, meaning they are subject to the law's requirements.

Organizations Likely to Be HIPAA-Covered Entities:

- **Health Plans:** These include insurance companies, health maintenance organizations (HMOs), and Medicaid and Medicare programs.
- **Healthcare Providers:** This encompasses doctors, hospitals, clinics, nursing homes, and dentists.
- **Healthcare Clearinghouses:** These organizations process claims between healthcare providers and payers.

Organizations Not Likely to Be HIPAA-Covered Entities:

- **Life Insurers:** While they may handle health information, they are generally not considered HIPAA-covered entities unless they provide healthcare services.

- **Disability Insurers:** Similar to life insurers, they are typically not subject to HIPAA if they don't offer healthcare services.
- **Work Comp Insurers:** These insurers usually handle health information related to workplace injuries, but they may not be covered under HIPAA.

Individuals Not Typically Covered:

- **Patients:** While patients have rights under HIPAA, they are not considered covered entities.
- **Family Members:** Unless they are authorized to act as the patient's representative, family members are not subject to HIPAA.

Note: It's essential to consult with legal counsel to determine if a specific organization or individual falls under HIPAA jurisdiction, as there can be exceptions and nuances depending on the circumstances.

OCR and FTC:

The Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) both play crucial roles in overseeing compliance with HIPAA regulations, but their specific responsibilities differ.

Office for Civil Rights (OCR):

- Enforcement: OCR is primarily responsible for enforcing HIPAA's privacy and security rules. They investigate complaints, conduct audits, and can impose civil monetary penalties on non-compliant entities.
- Education and Outreach: OCR also provides educational resources and guidance to help covered entities understand and comply with HIPAA regulations.
- Technical Assistance: OCR offers technical assistance to covered entities, helping them develop and implement compliance programs.

Federal Trade Commission (FTC):

- Unfair or Deceptive Trade Practices: The FTC's focus is on preventing unfair or deceptive trade practices. In the context of HIPAA, this means they may investigate and take action against entities that violate HIPAA regulations through deceptive marketing or advertising practices related to health information.
- Consumer Protection: The FTC also works to protect consumers' rights and interests. This includes ensuring that individuals have access to their health information and that it is protected from unauthorized use or disclosure.

Key Differences:

While both OCR and FTC are involved in HIPAA oversight, their primary areas of focus differ:

- OCR: Enforcement of HIPAA regulations, education, and technical assistance.

- FTC: Prevention of unfair or deceptive trade practices related to health information and consumer protection.

In some cases, OCR and FTC may collaborate on investigations or enforcement actions, particularly when there are overlapping issues involving both HIPAA compliance and consumer protection.

How to File a Complaint

Apps are subject to other Privacy laws. For example, the Federal Trade Commission Act (FTC) protects you against any App that breaks privacy rules. If an App breaks a privacy rule, the App may be held accountable by the federal government.

If you think your healthcare data have been breached or an app has used your data inappropriately you can file a complaint to LACDMH Patients' Rights Office. Please visit the following page for more information:
https://dmh.lacounty.gov/our-services/patients-rights/

You can also submit a complaint to OCR or FTC. For more information see below:

Office for Civil Rights (OCR):

To learn more about filing a complaint with OCR under HIPAA, visit:
https://www.hhs.gov/hipaa/filing-a-complaint/index.html

1. **Online Complaint Form:** The most convenient way to submit a complaint to OCR is through their online form. Individuals can file a complaint with OCR using the OCR complaint portal: https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf

2. **Mail:** You can also submit a complaint by mail to:

   Office for Civil Rights
   U.S. Department of Health and Human Services
   200 Independence Avenue, S.W.
   Washington, D.C. 20201

3. **Call:** You can also contact the OTC at Toll Free Call Center: 1-877-696-6775

Federal Trade Commission (FTC):

1. **Online Complaint Form:** To submit a complaint online through the FTC's website, please visit: https://www.ftc.gov/
   You can use FTC complaint assistant to file a complaint at FTC:

https://www.ftccomplaintassistant.gov/#crnt&panel1-1

2. **Mail:** You can also mail your complaint to:

   Bureau of Consumer Protection
   Federal Trade Commission
   600 Pennsylvania Ave., NW
   Washington, DC 20580

3. **Call:** You can also contact the FTC Consumer Response Center by calling 1-877-FTC-HELP (382-4357)

Important Tips on Filing a Complaint:

- **Be specific:** Provide as much detail as possible about the alleged violation, including dates, names, and any relevant documentation.
- **Keep a copy:** Make a copy of your complaint for your records.
- **Follow up:** If you don't receive a response within a reasonable time, you may want to follow up with the agency.

|End of the Document|