

San Benito County Patient Access API Member Educational Resources

Protecting your Privacy and Security

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. Patient Access API that allows communication between an electronic health record system and a 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 subset of their clinical information through third-party applications of their choice.

PRIVACY and SECURITY:

Patient Access API will allow the sharing of your health data with the third party App you'll choose. However, San Benito County Behavioral Health 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 health 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.

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.

Apps and HIPAA:

HIPAA 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](https://www.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>

Is 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:

- 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 noncompliant 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.

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 has been breached or an app has used your data inappropriately you can file a grievance with San Benito County Behavioral Health. Please visit the following page for more information:

<https://www.sanbenitocountyca.gov/home/showdocument?id=5591>

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 OCR 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://reportfraud.ftc.gov/assistant>
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.

Recursos educativos para miembros de la API de Acceso para Pacientes del Condado de San Benito

Protegiendo su privacidad y seguridad

¿Qué es una API?

Es una forma sencilla de que dos programas informáticos se comuniquen para obtener datos. Un ejemplo es cuando envía un mensaje usando un teléfono celular. La API de Acceso para Pacientes permite la comunicación entre un sistema de historial médico electrónico y una aplicación de terceros para recuperar datos de salud.

¿Qué son los datos de salud?

Los datos de salud son información sobre su historial médico, tratamiento para trastornos por consumo de sustancias, salud mental, estado de VIH u otra información confidencial. Puede incluir información demográfica, información sobre pruebas médicas, afecciones médicas, entre otros. También incluye información sobre reclamos y consultas, incluyendo costos, específicamente remesas a proveedores y costos compartidos de los afiliados, así como un subconjunto definido de su información clínica a través de aplicaciones de terceros de su elección.

PRIVACIDAD Y SEGURIDAD:

La API de Acceso para Pacientes le permitirá compartir sus datos de salud con la aplicación de terceros que elija. Sin embargo, el Departamento de Salud Conductual del Condado de San Benito no tiene control sobre cómo su aplicación usará o compartirá sus datos de salud.

Para proteger la privacidad y la seguridad de sus datos de salud, siga las siguientes pautas:

Qué buscar al elegir una aplicación de terceros:

Su aplicación tendrá acceso a todos sus datos de salud una vez que usted lo autorice. Debe leer la política de privacidad de su aplicación para ver cómo esta podría usar sus datos. Asegúrese de estar conforme con sus normas. Una aplicación que publica un aviso de privacidad debe cumplir con lo estipulado en dicho aviso. En general, haga lo siguiente antes de tomar una decisión final sobre la elección de una aplicación:

- **Investigue y revise:** Busque aplicaciones con una sólida reputación en materia de seguridad y privacidad de datos.
- **Verifique las certificaciones:** Busque certificaciones como la de cumplimiento con la HIPAA, que indica que la aplicación cumple con estándares de seguridad específicos.
- **Lea las políticas de privacidad:** Revise atentamente la política de privacidad para comprender cómo la aplicación recopila, usa y protege sus datos.

Antes de elegir una aplicación de terceros, le recomendamos revisar la siguiente lista de preguntas para tomar una decisión informada:

- ¿Qué datos de salud recopilará esta aplicación? ¿Recopilará esta aplicación datos no relacionados con la salud de mi dispositivo, como mi ubicación?
- ¿Mis datos se almacenarán de forma anónima?
- ¿Cómo utilizará esta aplicación mis datos? ¿Compartirá esta aplicación mis datos a terceros?
- ¿Venderá esta aplicación mis datos por algún motivo, como publicidad o investigación?

- ¿Compartiré esta aplicación mis datos por algún motivo? De ser así, ¿con quién? ¿Con qué propósito?
- ¿Su aplicación le permitirá controlar cómo puede usar sus datos?
- ¿Cómo puedo limitar el uso y la divulgación de mis datos por parte de esta aplicación?
- ¿Qué medidas de seguridad utiliza esta aplicación para proteger mis datos?
- ¿Qué impacto podría tener compartir mis datos con esta aplicación en otras personas, como mis familiares?
- ¿Cómo puedo acceder a mis datos y corregir inexactitudes en los datos recuperados por esta aplicación? ¿Esta aplicación cuenta con un proceso para recopilar y responder a las quejas de los usuarios?
- Si ya no quiero usar esta aplicación o si ya no quiero que tenga acceso a mi información médica, ¿cómo puedo cancelar el acceso de la aplicación a mis datos?
- ¿Cuál es la política de la aplicación para eliminar mis datos una vez que cancelo el acceso? ¿Tengo que hacer algo más que simplemente eliminar la aplicación de mi dispositivo?
- ¿Cómo informa esta aplicación a los usuarios sobre los cambios que podrían afectar sus prácticas de privacidad?

Si la política de privacidad de la aplicación no responde claramente a las preguntas anteriores, debería reconsiderar su uso. Dado que los datos de salud son muy sensibles, elija una aplicación con estándares de privacidad y seguridad sólidos para protegerlos.

Aplicaciones e HIPAA:

HIPAA es la Ley de Portabilidad y Responsabilidad del Seguro Médico. Esta es una ley federal que establece que su información médica no se puede compartir a menos que sea para tratamiento, pago u operaciones de atención médica, u otros motivos permitidos por la ley federal. La Oficina de Derechos Civiles (OCR) del Departamento de Salud y Servicios Humanos de EE. UU. (HHS) aplica las Normas de Privacidad, Seguridad y Notificación de Infracciones de la HIPAA, así como la Ley y Norma de Seguridad del Paciente. Para obtener más información sobre sus derechos bajo la HIPAA, visite [HHS.gov](https://www.hhs.gov).

La mayoría de las aplicaciones de terceros no están cubiertas por la HIPAA. En cambio, se encuentran bajo la jurisdicción de la Comisión Federal de Comercio (FTC) y las protecciones que brinda la Ley de la FTC. La Ley de la FTC, entre otras cosas, protege contra actos engañosos (por ejemplo, si una aplicación comparte datos personales sin permiso, a pesar de tener una política de privacidad que lo prohíbe). La FTC proporciona información sobre la privacidad y seguridad de las aplicaciones móviles para los consumidores aquí: <https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps>

¿Es seguro compartir datos de salud en línea?

Al tomar decisiones sobre su salud, solo debe compartir sus datos con personas y aplicaciones de confianza. Esto incluye a su familia, médicos u otras personas que consulte o en quienes confíe para recibir atención. Nunca comparta su nombre de usuario ni contraseña. Utilice únicamente software de confianza y siempre use una contraseña en su teléfono, tableta o computadora. No envíe datos por correo electrónico a menos que pueda protegerlos con una contraseña. Para obtener más información sobre seguridad en línea, consulte: Seguridad en Línea de la Comisión Federal de Comercio (FTC).

Nota: Los menores de 13 años no pueden compartir sus datos de salud a menos que sus padres, tutores u otro representante personal lo autoricen.

Consejos para mantener la información segura:

- Utilice únicamente aplicaciones de salud de confianza.
- Mantenga la privacidad de sus contraseñas e información de inicio de sesión.
- Guarde sus documentos privados en un lugar seguro.
- Adquiera un antivirus para su computadora.

Entidades Cubiertas por la HIPAA: Un Desglose

Ciertas organizaciones e individuos se consideran entidades cubiertas por la HIPAA, lo que significa que están sujetos a los requisitos de la ley.

Organizaciones que Probablemente Estén Cubiertas por la HIPAA:

- **Planes de Salud:** Incluyen compañías de seguros, organizaciones para el mantenimiento de la salud (HMO) y programas de Medicaid y Medicare.
- **Proveedores de Servicios de Salud:** Abarca médicos, hospitales, clínicas, residencias de ancianos y dentistas.
- **Centros de Intercambio de Información sobre Servicios de Salud:** Estas organizaciones procesan reclamaciones entre proveedores de servicios de salud y pagadores.

Organizaciones que Probablemente No Estén Cubiertas por la HIPAA:

- **Aseguradoras de Vida:** Si bien pueden manejar información médica, generalmente no se consideran entidades cubiertas por la HIPAA a menos que presten servicios de salud.
- **Aseguradoras de Discapacidad:** Al igual que las aseguradoras de vida, generalmente no están sujetas a la HIPAA si no ofrecen servicios de salud.
- **Aseguradoras de Compensación Laboral:** Estas aseguradoras suelen gestionar información médica relacionada con lesiones laborales, pero podrían no estar cubiertas por la HIPAA.

Individuos que no suelen estar cubiertos:

- **Pacientes:** Si bien los pacientes tienen derechos bajo la HIPAA, no se consideran entidades cubiertas.
- **Familiares:** A menos que estén autorizados para actuar como representantes del paciente, los familiares no están sujetos a la HIPAA.

Nota: Es fundamental consultar con un asesor legal para determinar si una organización o persona específica está sujeta a la jurisdicción de la HIPAA, ya que puede haber excepciones y matices según las circunstancias.

OCR y FTC:

La Oficina de Derechos Civiles (OCR) y la Comisión Federal de Comercio (FTC) desempeñan un papel crucial en la supervisión del cumplimiento de las regulaciones de la HIPAA, pero sus responsabilidades específicas difieren.

Oficina de Derechos Civiles (OCR):

- **Cumplimiento:** La OCR es la principal responsable de hacer cumplir las normas de privacidad y seguridad de la HIPAA. Investiga quejas, realiza auditorías y puede imponer sanciones económicas civiles a las entidades que incumplen.
- **Educación y Difusión:** La OCR también proporciona recursos educativos y orientación para ayudar a las entidades sujetas a la ley a comprender y cumplir con las regulaciones de la HIPAA.
- **Asistencia Técnica:** La OCR ofrece asistencia técnica a las entidades sujetas, ayudándolas a desarrollar e implementar programas de cumplimiento.

Comisión Federal de Comercio (FTC):

- **Prácticas Comerciales Desleales o Engañosas:** La FTC se centra en prevenir las prácticas comerciales desleales o engañosas. En el contexto de la HIPAA, esto significa que pueden investigar y tomar medidas contra las entidades que infrinjan las regulaciones de la HIPAA mediante prácticas de marketing o publicidad engañosas relacionadas con la información de salud.
- **Protección del Consumidor:** La FTC también trabaja para proteger los derechos e intereses de los consumidores. Esto incluye garantizar que las personas tengan acceso a su información de salud y que esta esté protegida contra el uso o la divulgación no autorizados.

Si bien tanto la OCR como la FTC participan en la supervisión de la HIPAA, sus principales áreas de enfoque difieren:

- **OCR:** Aplicación de las regulaciones de la HIPAA, educación y asistencia técnica.
- **FTC:** Prevención de prácticas comerciales desleales o engañosas relacionadas con la información de salud y protección del consumidor.

En algunos casos, la OCR y la FTC pueden colaborar en investigaciones o acciones de cumplimiento, especialmente cuando existen problemas comunes relacionados con el cumplimiento de la HIPAA y la protección del consumidor.

Cómo presentar una queja

Las aplicaciones están sujetas a otras leyes de privacidad. Por ejemplo, la Ley de la Comisión Federal de Comercio (FTC) lo protege contra cualquier aplicación que infrinja las normas de privacidad. Si una aplicación incumple una norma de privacidad, el gobierno federal podría exigirle responsabilidades.

Si cree que sus datos médicos han sido vulnerados o que una aplicación los ha utilizado de forma inapropiada, puede presentar una queja ante el Departamento de Salud Conductual del Condado de San Benito. Visite la siguiente página para obtener más información:

<https://www.sanbenitocountyca.gov/home/showdocument?id=5591>

También puede presentar una queja ante la OCR o la FTC. Para más información, consulte a continuación:

Oficina de Derechos Civiles (OCR):

Para obtener más información sobre cómo presentar una queja ante la OCR bajo la HIPAA, visite: <https://www.hhs.gov/hipaa/filing-a-complaint/index.html>

1. Formulario de queja en línea: La forma más conveniente de presentar una queja ante la OCR es a través de su formulario en línea. Puede presentar una queja ante la OCR a través del portal de quejas de la OCR:

<https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>

2. Correo postal: También puede enviar una queja por correo postal a:

Oficina de Derechos Civiles, Departamento de Salud y Servicios Humanos de EE. UU., 200 Independence Avenue, S.W. Washington, D.C. 20201

3. Llamada: También puede contactar a la OCR a través del Centro de Llamadas Gratuito: 1-877-696-6775

Comisión Federal de Comercio (FTC):

1. Formulario de Queja en Línea: Para presentar una queja en línea a través del sitio web de la FTC, visite: <https://www.ftc.gov/>

Puede utilizar el asistente de quejas de la FTC para presentar una queja:
<https://reportfraud.ftc.gov/assistant>

2. Correo: También puede enviar su queja por correo a: Oficina de Protección al Consumidor, Comisión Federal de Comercio, 600 Pennsylvania Ave., NW, Washington, D.C. 20580

3. Llamada: También puede contactar al Centro de Respuesta al Consumidor de la FTC llamando al 1-877-FTC-HELP (382-4357)