



Interoperabilidad y protección de tu información de salud

Centers for Medicare & Medicaid Services (CMS) publicó la Regla Final sobre Interoperabilidad y Acceso del Paciente el 1 de mayo de 2020. Esta regla final se centra en impulsar la interoperabilidad y el acceso de los pacientes a la información de salud, poniendo a los pacientes en primer lugar, dándote acceso a tu información de salud cuando más la necesitas y de una forma que te resulte más útil.

Esta normativa incluye políticas que exigen o fomentan que los pagadores, como Amida Care, implementen Interfaces de Programación de Aplicaciones (Application Programming Interfaces, API) para mejorar el intercambio electrónico de datos de salud, ya sea compartiendo información contigo o intercambiando información entre un pagador y un proveedor, o entre dos pagadores.

Esta norma te da acceso y uso de tu historia clínica electrónica (electronic health record, EHR) completa, la tranquilidad de que tus proveedores de salud están comunicándose y coordinando tu atención, y la posibilidad de involucrarte en tu propio cuidado de una manera más significativa.

¿Qué significa todo esto? Esto significa que, **con tu consentimiento**, Amida Care podría compartir tus registros de salud con aplicaciones de terceros (apps), para hacer que el intercambio de tu información de salud sea más accesible para ti, tus proveedores y tus aseguradoras de salud. Amida Care solo **compartirá tu información de salud electrónica** con un desarrollador de aplicaciones de terceros **si nos lo solicitas**.

Una vez que le das permiso a Amida Care para compartir tu información de salud electrónica con una aplicación de terceros, es importante que sepas que Amida Care **ya no es responsable** de los datos una vez que la app los recibe. Esto significa que Amida Care no es responsable de cómo la app utiliza tus datos ni de cómo los protege. También significa que, una vez que das tu consentimiento para divulgar tu historia clínica electrónica a una app de terceros, la información que reciba la app puede dejar de estar cubierta por la Ley de Portabilidad y Responsabilidad de Seguros de Salud (Health Insurance Portability and Accountability Act, HIPAA), ya que la mayoría de los desarrolladores de aplicaciones de terceros no se consideran una “entidad cubierta” bajo HIPAA. Para obtener más información sobre HIPAA y quiénes están obligados a cumplirla, **haz clic [aquí](#)**. Para ver las **preguntas frecuentes sobre HIPAA**, **haz clic [aquí](#)**.



Interoperabilidad y protección de tu información de salud

Es importante que leas detenidamente cualquier aviso de privacidad y seguridad emitido por la aplicación **antes de dar tu consentimiento para que Amida Care divulgue tu información de salud electrónica a una app**. Según la Comisión Federal de Comercio (Federal Trade Commission, FTC), el desarrollador de la aplicación también debe informar cómo comparte la información sensible en la documentación de su producto.

¿Las aplicaciones de terceros están cubiertas por HIPAA?

La mayoría de las aplicaciones de terceros no están cubiertas por HIPAA. En su lugar, la mayoría de estas aplicaciones quedan bajo la jurisdicción de la FTC y las protecciones que brinda la Ley de la FTC. Esta ley, entre otras cosas, protege contra prácticas engañosas (por ejemplo, si una app comparte datos personales sin permiso, a pesar de tener una política de privacidad que indica que no lo hará). La FTC ofrece información sobre la privacidad y seguridad de las aplicaciones móviles para los consumidores [*aquí*](#).

¿Qué aspectos importantes debes considerar antes de autorizar a una aplicación de terceros a acceder a tus datos de atención médica?

Es importante que **asumas un rol activo en la protección de tu información de salud** y que **elijas con cuidado aplicaciones que cuenten con sólidos estándares de privacidad y seguridad**. Si una aplicación no tiene una política de privacidad, Centers for Medicare & Medicaid Services (CMS) recomienda que no la utilices. La política de privacidad de la aplicación debe responder claramente a las siguientes preguntas:

- ¿Qué datos de salud recopilará esta aplicación? ¿Recopilará también datos no relacionados con la salud desde mi dispositivo, como mi ubicación?
- ¿Mis datos se almacenarán de forma desidentificada o anonimizada?
- ¿Cómo utilizará esta aplicación mis datos?
- ¿Esta aplicación divulgará o venderá mis datos a terceros?
 - ¿Esta aplicación venderá mis datos por algún motivo, como publicidad o investigación?
 - ¿Esta aplicación compartirá mis datos por algún motivo? En caso afirmativo, ¿con quién? ¿Con qué propósito?

Interoperabilidad y protección de tu información de salud

- ¿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 el hecho de compartir mis datos con esta aplicación en otras personas, como mis familiares?
- ¿Cómo puedo acceder a mis datos y corregir inexactitudes en los datos que esta aplicación haya obtenido?
- ¿Esta aplicación cuenta con un proceso para recibir y responder a las quejas de los usuarios?
- Si ya no quiero utilizar esta aplicación o si ya no quiero que tenga acceso a mi información de salud, ¿cómo puedo revocar su acceso a mis datos?
 - ¿Cuál es la política de la aplicación para eliminar mis datos una vez que revoque el acceso? ¿Debo hacer algo más que simplemente eliminar la aplicación de mi dispositivo?
- ¿Cómo informa esta aplicación a los usuarios sobre cambios que puedan afectar sus prácticas de privacidad?

Si la política de privacidad de la aplicación no responde claramente a estas preguntas, CMS indica que deberías reconsiderar el uso de la app para acceder a tu información de salud. **La información de salud es muy sensible, por lo que debes ser cuidadoso al elegir aplicaciones que cuenten con sólidos estándares de privacidad y seguridad para protegerla.**

¿Qué debe hacer un paciente si cree que sus datos han sido vulnerados o que una aplicación ha utilizado sus datos de manera inapropiada?

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

Las personas pueden presentar una queja ante la OCR a través del portal de quejas de la OCR: <https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>

Las personas pueden presentar una queja ante la FTC mediante el asistente de quejas de la FTC: <https://reportfraud.ftc.gov/#/>



Interoperabilidad y protección de tu información de salud

Para obtener más información sobre las prácticas de privacidad de Amida Care y cómo contactarnos, visita:

<https://www.amidacareny.org/wp-content/uploads/ac-notice-V4.pdf>