U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

Preguntas frecuentes sobre telemedicina y sobre la ley HIPAA durante la emergencia nacional de salud pública por el COVID-19

1. ¿Qué es la telemedicina?

La Administración de Recursos y Servicios de Salud (HRSA, por sus siglas en inglés) del Departamento de Salud y Servicios Humanos de Estados Unidos (HHS, por sus siglas en inglés) define la telemedicina como el uso de información electrónica y de tecnologías de las telecomunicaciones para facilitar y promover la atención médica clínica a distancia, la educación de salud profesional y para pacientes, la salud pública y la administración de salud. Las tecnologías incluyen las videoconferencias, la Internet, el almacenamiento y el envío de estudios de diagnóstico por imágenes, los medios de transmisión en línea, el teléfono fijo y las comunicaciones inalámbricas.

Los servicios de telemedicina pueden prestarse, por ejemplo, mediante archivos de audio, mensajes de texto o tecnologías de comunicación por video, como un programa de videoconferencias. Por fines relacionados con reembolsos, algunos pagadores, como Medicare y Medicaid, pueden imponer restricciones en los tipos de tecnologías que se pueden usar[1]. Dichas restricciones no limitan el alcance de la Notificación de Discreción de Cumplimiento de la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA, por sus siglas en inglés) sobre el COVID-19 y las comunicaciones remotas de telemedicina.

2. ¿Qué entidades están incluidas y cuáles excluidas en virtud de la Notificación de Discreción de Cumplimiento sobre el COVID-19 y las comunicaciones remotas de telemedicina?

La Notificación de Discreción de Cumplimiento emitida por la Oficina de Derechos Civiles (OCR, por sus siglas en inglés) del HHS se aplica a todos

[1] Medicare paga muchos servicios diferentes que involucran el uso de estos tipos de tecnologías de la comunicación. Puede encontrar una hoja informativa sobre el pago y la cobertura de Medicare en https://www.cms.gov/files/document/03052020-medicare-covid-19-fact-sheet.pdf. Los servicios de telemedicina que paga Medicare son los servicios definidos en el artículo 1834(m) de la Ley del Seguro Social (Social Security Act) que, en otras circunstancias, se prestarían en persona, pero que ahora se prestan mediante tecnologías de la comunicación en tiempo real e interactivas.

los proveedores de atención médica que estén cubiertos por la ley HIPAA y que presten servicios de telemedicina durante la emergencia. Una compañía de seguros médicos que paga los servicios de telemedicina no está cubierta por la Notificación de Discreción de Cumplimiento.

En virtud de la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA, por sus siglas en inglés), un "proveedor de atención médica" es un proveedor de servicios médicos o de salud, y cualquier otra persona u organización que facilite servicios de atención médica, los facture o reciba un pago por ellos en el curso normal de su actividad. Los proveedores de atención médica comprenden, por ejemplo, médicos, enfermeros, clínicas, hospitales, asistentes de atención médica a domicilio, terapeutas, otros profesionales de salud mental, dentistas, farmacéuticos, laboratorios, y cualquier otra persona o entidad que dé atención médica. Un "proveedor de atención médica" es una entidad cubierta en virtud de la ley HIPAA si transmite cualquier tipo de información médica en formato electrónico en relación con una transacción para la cual la Secretaría haya adoptado un estándar (por ejemplo, la facturación electrónica de los seguros médicos). Consulte el artículo 160.103 del Título 45 del Código de Regulaciones Federales (CFR, por sus siglas en inglés) (45 CFR 160.103) (definiciones de *proveedor de atención médica*, *atención médica* y *entidad cubierta*).

Por el contrario, una compañía de seguros médicos que solo paga los servicios de telemedicina no estaría cubierta por la Notificación de Discreción de Cumplimiento porque no presta servicios de atención médica.

3. ¿Qué pacientes puede tratar un proveedor de atención médica cubierto en virtud de la Notificación de Discreción de Cumplimiento sobre el COVID-19 y las comunicaciones remotas de telemedicina? ¿Están incluidos los pacientes que tienen Medicare y Medicaid?

Esta Notificación se aplica a todos los proveedores de atención médica cubiertos por la ley HIPAA, y no se limita a los pacientes a los que atiendan mediante servicios de telemedicina, incluidos los pacientes que reciben beneficios de Medicare o Medicaid, y aquellos que no los reciben.

Hay información específica sobre los servicios de telemedicina y Medicare en https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet y en https://edit.cms.gov/files/document/medicare-telehealth-frequently-asked-questions-faqs-31720.pdf.

4. ¿Qué partes de las Normas de la ley HIPAA están incluidas en la Notificación de Discreción de Cumplimiento sobre el COVID-19 y las comunicaciones remotas de telemedicina?

Los proveedores de atención médica cubiertos no recibirán sanciones por violaciones de las Normas de la ley HIPAA sobre la privacidad, la seguridad y la notificación del incumplimiento que se produzcan mientras presten servicios de telemedicina de buena fe durante la emergencia nacional de salud pública por el COVID-19. Esta Notificación no afecta la aplicación de las Normas de la ley HIPAA en otras áreas de la atención médica aparte de la telemedicina durante la emergencia.

5. ¿La Notificación de Discreción de Cumplimiento sobre el COVID-19 y las comunicaciones remotas de telemedicina se aplica a las violaciones de la Parte 2 del Título 42 del CFR, la norma del HHS que protege la confidencialidad de los expedientes de los pacientes con trastornos por consumo de sustancias?

No, la Notificación solo aborda el cumplimiento de las Normas de la ley HIPAA. La Administración de Servicios de Salud Mental y Abuso de Sustancias (SAMHSA, por sus siglas en inglés) ha publicado una directriz similar sobre el COVID-19 y la Parte 2 del Título 42 del CFR, que está disponible en https://www.samhsa.gov/sites/default/files/covid-19-42-cfr-part-2-guidance-03192020.pdf.

6. ¿Cuándo vence la Notificación de Discreción de Cumplimiento sobre el COVID-19 y las comunicaciones remotas de telemedicina?

Esta Notificación no tiene fecha de vencimiento. La OCR publicará un aviso para el público cuando ya no ejerza su discreción de cumplimiento en función de los últimos datos y circunstancias.

7. ¿Dónde pueden los proveedores de atención médica prestar los servicios de telemedicina?

La OCR prevé que los proveedores de atención médica, por lo general, presten los servicios de telemedicina en lugares privados, por ejemplo, desde una clínica o un consultorio, un médico puede comunicarse con un paciente que esté en su casa o en otra clínica. Los proveedores siempre deben usar lugares privados, y los pacientes no deben recibir los servicios de telemedicina en lugares públicos o semipúblicos, sin dar su consentimiento ni en circunstancias apremiantes.

Si no se pueden prestar los servicios de telemedicina en un lugar privado, los proveedores de atención médica cubiertos deben seguir implementando

medidas de protección razonables en función de la ley HIPAA para limitar las posibilidades de que se use o se revele información de salud protegida (PHI, por sus siglas en inglés) de manera accidental. Dichas medidas de precaución razonables podrían incluir hablar en voz baja, no usar altavoz o recomendar que el paciente se aleje razonablemente de otras personas cuando hablen sobre PHI.

8. ¿Qué servicios de telemedicina están cubiertos por la Notificación de Discreción de Cumplimiento sobre el COVID-19 y las comunicaciones remotas de telemedicina?

Esta Notificación cubre todos los servicios que un proveedor de atención médica, según su criterio profesional, considere que se pueden prestar mediante telemedicina en las circunstancias de la emergencia actual. Esto incluye el diagnóstico o el tratamiento de las afecciones relacionadas con el COVID-19, por ejemplo, tomarle la temperatura o los signos vitales al paciente a la distancia, y el diagnóstico y el tratamiento de afecciones no relacionadas con el COVID-19, como revisar las prácticas de fisioterapia, administrar terapia de salud mental o modificar las recetas de medicamentos, entre otras cosas.

9. ¿Qué podría constituir "mala fe" en la prestación de servicios de telemedicina por parte de un proveedor de atención médica cubierto, lo cual no estaría cubierto por la Notificación de Discreción de Cumplimiento sobre el COVID-19 y las comunicaciones remotas de telemedicina?

La OCR considerará todos los hechos y las circunstancias a la hora de determinar si un proveedor de atención médica proporcionó los servicios de telemedicina de buena fe y, por lo tanto, si está cubierto por el Aviso. Algunos ejemplos de lo que la OCR puede considerar una "prestación de servicios de telemedicina de mala fe" que no estará cubierta por este Aviso son los siguientes:

- Cometer o fomentar un delito, como fraude, robo de identidad e invasión intencional de la privacidad.
- Volver a usar o a revelar los datos de un paciente trasmitidos durante una comunicación de telemedicina en los casos prohibidos por la Norma de Privacidad de la ley HIPAA (por ejemplo, vender datos o usarlos con fines de marketing sin autorización).
- Incumplir las leyes estatales de acreditación o los estándares de ética profesional, por lo cual se generen medidas disciplinarias relacionadas con el tratamiento ofrecido o proporcionado por telemedicina (es decir, basado en los resultados documentados de una junta de acreditación de atención médica o una junta de ética profesional).

- Usar productos de comunicación remota disponible para el público general, como TikTok, Facebook Live, Twitch o una sala de chat pública, que la OCR haya identificado en la Notificación como formas inaceptables de comunicación remota para la telemedicina porque están diseñadas para ser abiertas al público o porque permiten un acceso amplio o indiscriminado a la comunicación.

10. ¿Qué es un producto de comunicación remota "no disponible para el público general"?

Un producto de comunicación remota "no disponible para el público general" es un producto que, por defecto, permite que solo las partes deseadas participen en la comunicación.

Se incluyen, por ejemplo, las plataformas como FaceTime de Apple, videochat de Facebook Messenger, videos de Hangouts de Google, videochat de WhatsApp, Zoom, o Skype. Dichos productos también incluirían las aplicaciones de mensajes de texto que se usan habitualmente, como Signal, Jabber, Facebook Messenger, Hangouts de Google, WhatsApp o iMessage. Por lo general, estas plataformas emplean una encriptación de un extremo a otro, lo que permite que solo una persona y la otra con la que se comunica vean lo que se transmite.

Las plataformas también ofrecen cuentas de usuarioejercer cierto grado s individuales, accesos y contraseñas para ayudar a limitar el acceso y hacer una verificación de los participantes. Además, los participantes pueden ejercer cierto grado de control respecto de algunas funciones particulares, como elegir grabar o no la comunicación, silenciar el micrófono o apagar la cámara o la señal de audio en cualquier momento.

Por el contrario, los productos de comunicación remota disponible para el público general, como TikTok, Facebook Live, Twitch o una sala de chat pública, no son formas aceptables de comunicación remota para la telemedicina porque están diseñadas para ser abiertas al público o porque permiten un acceso amplio o indiscriminado a la comunicación. Por ejemplo, si un proveedor usa Facebook Live para transmitir una presentación disponible para todos sus pacientes sobre los riesgos de el COVID-19, no se considerará que presta servicios de telemedicina de manera razonablemente privada. Si un proveedor decide hacer una presentación mediante un producto de comunicación remota disponible para el público general, no estará cubierto por la Notificación, y no debería identificar a los pacientes ni ofrecerles asesoramiento personalizado en dicha transmisión en vivo.

11. Si un proveedor de atención médica cubierto presta servicios de telemedicina durante el brote del COVID-19 y, durante la transmisión, se intercepta información de salud protegida en formato electrónico, ¿la OCR sancionará al proveedor por violar la Norma de Seguridad de la ley HIPAA?

No. La OCR ejercerá su discreción de cumplimiento y no impondrá sanciones, que serían aplicables en otros contextos, por el incumplimiento que se produzca a partir de la prestación de servicios de telemedicina de buena fe durante la emergencia nacional de salud pública por el COVID-19. La OCR considerará todos los hechos y las circunstancias a la hora de determinar si los servicios de telemedicina se prestaron de buena fe. Por ejemplo, si un proveedor cumple los términos de la Notificación y cualquier directriz vigente de la OCR (como esta y otras preguntas frecuentes sobre el COVID-19 y la ley HIPAA), no recibirá sanciones en virtud de la ley HIPAA si le hackean la transmisión y se expone la información de salud protegida de una sesión de telemedicina.

La OCR cree que muchos productos electrónicos de comunicación remota que actualmente se usan de manera habitual incluyen funciones de seguridad para proteger la PHI electrónica (ePHI, por sus siglas en inglés) que se transmite entre los proveedores de atención médica y los pacientes. Asimismo, los proveedores de comunicación por video que conocen los requisitos de la Norma de Seguridad suelen incluir funciones de seguridad más fuertes para evitar la interceptación de datos y garantizar que protegerán la ePHI, dado que firman un acuerdo de asociado de negocio (BAA, por sus siglas en inglés) de la ley HIPAA. A los proveedores que deseen usar productos de comunicación por video se les recomienda usar dichos proveedores de comunicación, pero no se los sancionará por usar productos menos seguros con el fin de prestar la atención más oportuna y accesible posible para los pacientes durante la emergencia de salud pública. Se recomienda que los proveedores les avisen a los pacientes que estas aplicaciones de terceros podrían presentar riesgos de privacidad. Además, los proveedores deben habilitar todos los modos de encriptación y privacidad disponibles al usar dichas aplicaciones.

La OCR no avala el uso ni las funciones de seguridad de ningún producto de comunicación particular.