



Política de privacidad de Included Health

Fecha de entrada en vigencia: 1.º de febrero de 2026

Esta política describe cómo Included Health, Inc. y sus entidades asociadas ("Included Health", "nosotros", "nos", "nuestro(s)" o "nuestra(s)") recopilan, utilizan, divulgan y protegen la información personal a través de nuestros sitios web, aplicaciones móviles, y productos y servicios que contienen enlaces a la presente Política de Privacidad (en conjunto, los "Sitios").

Nuestro propósito es:

- garantizar una clara comprensión de cómo Included Health procesa la información personal y relacionada con la salud;
- demostrar el cumplimiento con la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA, por sus siglas en inglés), la Ley de Privacidad del Consumidor de California (CCPA, por sus siglas en inglés) y la Ley de Derechos de Privacidad de California (CPRA, por sus siglas en inglés), así como otras leyes de privacidad aplicables en EE. UU.; y
- reafirmar el compromiso de Included Health con la transparencia, la confianza y la administración responsable de los datos.

Included Health, Inc. ("Included Health", la "Empresa", "nosotros", "nos", "nuestro(s)" o "nuestra(s)") opera los sitios web disponibles en includedhealth.com y doctorondemand.com, al igual que otros sitios web, productos, servicios y aplicaciones móviles con enlaces a la presente Política de privacidad, que incluyen de modo no taxativo las páginas web y aplicaciones seguras de Doctor On Demand (en conjunto, los "Sitios" o "Sitios web", a menos que se especifique lo contrario). En adelante, los usuarios de los Sitios o Servicios se denominan "Usuarios", "Miembros", "usted" o "su".

Nuestra empresa ofrece servicios de telemedicina en línea, mediante los cuales nuestros Miembros pueden informar su historia clínica y solicitar profesionales de salud independientes ("Profesionales de salud") para recibir servicios médicos y de salud, así como para obtener asesoramiento sobre conductas saludables de parte de Asesores ("Asesores"), quienes no brindan servicios profesionales o clínicos.

Los Profesionales de salud que prestan Servicios a través de Included Health son profesionales independientes que ejercen en el marco de diversos grupos de prácticas profesionales independientes (en conjunto, "Doctor On Demand Professionals"). Consulte el Aviso de prácticas de privacidad de Doctor On Demand Professionals para obtener más información sobre estos grupos y comprender cómo están organizados.

Tenga en cuenta que los Usuarios en diferentes regiones pueden estar sujetos a distintas leyes, regulaciones y normas en materia de protección de datos. Por lo tanto, el presente documento cuenta con una sección dedicada a los consumidores de California, así como con una sección dedicada a los consumidores bajo la jurisdicción de la Unión Europea.

Lea atentamente la presente Política de privacidad antes de utilizar los Sitios o Servicios. Al visitar o usar cualquiera de los Sitios o Servicios, usted acepta las prácticas descritas en la presente Política de privacidad, así como los Términos del servicio de Included Health y otros términos, acuerdos, declaraciones de derechos, formularios de consentimiento y políticas que se mencionaron anteriormente, según corresponda.

Alcance geográfico: Los servicios de Included Health están destinados a personas físicas ubicadas en Estados Unidos, y procesamos principalmente información personal de conformidad con las leyes aplicables de privacidad y atención médica de Estados Unidos. Si llegáramos a estar sujetos a leyes de protección de datos fuera de Estados Unidos en relación con usuarios, servicios o actividades de procesamiento específicos, cumpliremos con dichas leyes según corresponda.

Cobertura estadual: Esta política está diseñada para operaciones en los 50 estados de EE. UU. e incorpora mayores protecciones exigidas por las leyes estatales de privacidad aplicables.

1. Información que recopilamos

Recopilamos las siguientes categorías de datos de los Miembros, usuarios, empleadores y socios del plan de salud:

- Identificadores: nombre, dirección, correo electrónico, número de teléfono, fecha de nacimiento, número de Seguridad Social (solo los cuatro últimos dígitos, cuando sea necesario para la verificación de la identidad o la administración del plan y según lo permitido por la ley).
- Información demográfica y de elegibilidad: datos del empleador o del plan, información sobre la cobertura, elegibilidad para los beneficios y números de identificación del miembro.
- Información de salud: historia clínica, síntomas, diagnósticos, prescripciones, notas clínicas, datos de reclamos y correspondencia con proveedores.
- Datos técnicos y de uso: dirección IP, tipo de dispositivo, tipo de navegador, identificador móvil, cookies, balizas y otros datos analíticos.
- Datos de correspondencia y de interacción: mensajes, solicitudes de asistencia o interacciones por chat a través de nuestras aplicaciones o del portal para miembros.

Recopilamos datos directamente de usted, de su plan de salud o empleador (según lo permitan las leyes o el contrato), de sus profesionales de la salud y a través de tecnologías que respaldan nuestra plataforma.

2. Uso de la información

Utilizamos la información personal identificable (PII, por sus siglas en inglés) y la información de salud protegida (PHI, por sus siglas en inglés) para fines comerciales lícitos, los cuales incluyen:

- la prestación y la coordinación de servicios clínicos y de telemedicina;
- la gestión de las cuentas de los miembros y la atención al cliente;
- el procesamiento de pagos y de reclamos de seguros;
- la realización de análisis para las operaciones de atención médica, la mejora de la calidad, la gestión de la salud poblacional y la optimización de los servicios, según lo permitido por la HIPAA y la legislación aplicable;
- la comunicación sobre beneficios, programas y actualizaciones de servicios;
- la protección contra fraudes, amenazas a la seguridad o actividades ilícitas; y
- el cumplimiento de requisitos legales o normativos.

No utilizamos ni divulgamos la información de salud protegida para fines de marketing o venta sin su autorización.

3. Divulgación de información

Podemos compartir información de la siguiente manera:

Categoría	Finalidad
Con planes y proveedores de atención médica	Para tratamientos, pagos y operaciones de atención médica, conforme a la HIPAA.
Con proveedores y asociados de negocios	Para prestar servicios en nuestro nombre (por ejemplo, alojamiento, seguridad informática, soporte para reclamos). Todos los proveedores deben firmar Acuerdos de Asociados de Negocios y cumplir con las disposiciones de la HIPAA.
Con empleadores o patrocinadores de beneficios	Se limitará a datos agregados y desidentificados, salvo autorización expresa o cuando la ley lo permita o lo exija; no obstante, podrá utilizarse información a nivel individual cuando ello resulte necesario para administrar beneficios, coordinar la atención médica o cuando exista autorización del Miembro o requerimiento legal.
Con autoridades competentes de aplicación de la ley o regulatorias	Cuando así lo exija la ley, una orden judicial o una citación.
Para transacciones corporativas	En relación con una fusión, adquisición o transferencia de activos, y sujeto a las correspondientes obligaciones de confidencialidad.
Para fines legales y de cumplimiento normativo	Para hacer cumplir derechos, prevenir el fraude y cumplir con las leyes aplicables.

No vendemos datos de los Miembros y no compartimos la PHI con intermediarios de datos ni con plataformas publicitarias.

4. Cumplimiento de la HIPAA

Cuando Included Health actúa como entidad cubierta o asociado de negocios, gestionamos la PHI de acuerdo con las Normas de Privacidad, Seguridad y Notificación de Brechas de la HIPAA y nuestros Acuerdos de Asociados de Negocios.

Mantenemos controles de seguridad de conformidad con la HIPAA, que incluye el cifrado en tránsito y (cuando corresponda) en reposo, el registro de accesos, las auditorías y la capacitación de los empleados.

5. Derechos de privacidad de los consumidores en California y otros estados

Los residentes de ciertos estados tienen derechos adicionales. Para los residentes de California en virtud de la Ley de Privacidad del Consumidor de California (CCPA, por sus siglas en inglés) y la Ley de Derechos de Privacidad de California (CPRA, por sus siglas en inglés), así como para los residentes de otros estados con leyes comparables:

Usted puede tener derecho a:

- saber qué información personal recopilamos y cómo la utilizamos;

- solicitar acceso a su información personal o su eliminación;
- corregir información personal inexacta;
- solicitar la exclusión de la “venta” o el “intercambio” de información personal (de acuerdo con la legislación estadual aplicable); y
- limitar el uso de información personal sensible cuando lo exija la ley.

Included Health no vende información personal. Determinadas cookies de terceros o herramientas de analítica pueden constituir una “venta” o un “intercambio” de información personal conforme a la legislación estadual; los usuarios pueden optar por excluirse a través del enlace “No vender ni compartir mi información” disponible en nuestros Sitios. Asimismo, respetamos las señales de preferencia de exclusión cuando así lo exija la ley.

Las solicitudes para ejercer estos derechos deben ser verificables y presentarse a través de nuestro portal de privacidad o por correo electrónico a privacy@includedhealth.com. Responderemos dentro de los plazos legales aplicables (normalmente 45 días, prorrogables hasta 90 días mediante notificación previa).

Información personal sensible:

A los efectos de las leyes estaduais de privacidad aplicables (incluida la Ley de Derechos de Privacidad de California), la Información personal sensible (SPI, por sus siglas en inglés) incluye información personal que revele o que esté relacionada con:

- el número de Seguro Social de un consumidor, el número de su licencia de conducir, el número de su tarjeta de identificación estadual o el número de su pasaporte;
- las credenciales de inicio de sesión de la cuenta de un consumidor, el número de su cuenta financiera, tarjeta de débito o tarjeta de crédito, en combinación con cualquier código de seguridad o acceso, contraseña u otras credenciales que permitan el ingreso a una cuenta;
- la geolocalización precisa de un consumidor;
- el origen racial o étnico de un consumidor, sus creencias religiosas o filosóficas, o su afiliación sindical;
- el contenido de la correspondencia postal, el correo electrónico o los mensajes de texto de un consumidor, a menos que Included Health sea el destinatario previsto de la comunicación;
- los datos genéticos o la información biométrica de un consumidor para identificarlo de manera única; y
- la información de salud de un consumidor, incluidas las condiciones médicas, los diagnósticos, la información sobre tratamientos y otros datos supeditados a las disposiciones de la HIPAA u otras leyes similares de privacidad en materia de atención médica.

Cuando así lo exija la ley, usted podrá tener derecho a limitar el uso y la divulgación de la Información personal sensible a los fines permitidos por las leyes aplicables, como la prestación de servicios de atención médica, el mantenimiento de la seguridad de la cuenta, el cumplimiento de obligaciones legales y otros fines comerciales y operativos necesarios.

Apelaciones. Cuando la legislación estadual aplicable así lo requiera, usted podrá apelar nuestra decisión en relación con su solicitud sobre sus derechos de privacidad. Las instrucciones para presentar una apelación se proporcionarán junto con nuestra respuesta. Responderemos a las apelaciones dentro del plazo exigido por la ley.

6. Seguridad de los datos

Mantenemos salvaguardas administrativas, técnicas y físicas razonables para proteger la PII y la PHI frente al acceso o divulgación no autorizados, que incluyen:

- la autenticación multifactor y controles de acceso conforme al principio de mínimo privilegio;
- el monitoreo continuo y el cifrado de datos en tránsito y en reposo; la gestión de riesgos de proveedores y la debida diligencia en materia de seguridad;
- protocolos de respuesta ante incidentes y de notificación de brechas de seguridad; y
- la capacitación y evaluación anuales para los miembros del personal.

Ningún sistema es completamente seguro; sin embargo, seguimos las mejores prácticas vigentes del Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés) y del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) y llevamos a cabo evaluaciones de riesgo periódicas.

7. Conservación y destrucción de datos

La información personal se conserva solamente durante el tiempo necesario para darle el uso previsto, cumplir con las obligaciones legales, resolver las disputas y hacer cumplir los acuerdos. La PHI se conserva de acuerdo con los requisitos federales y estatales de conservación de registros. La documentación administrativa exigida por la HIPAA se conserva durante al menos seis años, y los registros médicos y clínicos se conservan de acuerdo con los requisitos federales y estatales aplicables de conservación de registros médicos, que pueden establecer plazos más extensos. Los datos se destruyen de forma segura o se desidentifican cuando ya no son necesarios.

8. Notificación de brechas de seguridad

Si se produce una brecha de PHI o PII no protegida, notificaremos a las personas afectadas y a los organismos reguladores sin demoras injustificadas y dentro de los plazos exigidos por la legislación federal y estatal aplicable. Los proveedores y asociados de negocios deberán informar sobre cualquier incidente a Included Health en un plazo de 24 horas desde su detección, de conformidad con la actualización de la Regla de Seguridad del HHS de 2025.

9. Responsabilidades del personal

Included Health mantiene programas de capacitación del personal y mecanismos internos de notificación para respaldar el cumplimiento de los requisitos de privacidad y seguridad.

10. Gobernanza y administración de la política

El Director de Cumplimiento (CCO, por sus siglas en inglés) supervisa esta política y aprueba las actualizaciones en consulta con los equipos de Asuntos Legales y Seguridad de la Información. El CCO lleva a cabo revisiones bienales (o con mayor frecuencia si se modifican las leyes) y supervisa la implementación a través de auditorías periódicas y evaluaciones de riesgos.

11. Ejercicio de los derechos de privacidad

Las solicitudes de acceso, corrección, eliminación o restricción de datos deberán presentarse a través del:

- Portal para Miembros (mediante el chat o la función de apertura de casos); o
- Correo electrónico a privacy@includedhealth.com, sujeto a los procedimientos de verificación de identidad.

Responderemos a las solicitudes de acceso conforme a la HIPAA en un plazo de 30 días, con una posibilidad de prórroga según lo permitido por la ley, y a las solicitudes de privacidad de los consumidores en un plazo de 45 días (prorrogables hasta 90 días mediante notificación previa).