

Notice of Privacy Practices

Effective Date: January 1, 2026

This Notice describes how Doctor On Demand Professionals may use and disclose your Protected Health Information (PHI) (referred to as “health information”) and how you, the patient, can get access to this information. Doctor On Demand Professionals is legally obligated to maintain the privacy of your health information and abide by applicable federal and state laws, including the Health Insurance Portability and Accountability Act (“HIPAA”).

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

1. Who we are

Clinical services provided on the Included Health or Doctor On Demand apps are provided by Doctor On Demand Professionals. Doctor On Demand Professionals is a group of independently owned professional entities associated with, but operationally independent from, Included Health, Inc. (“Included Health”). Clinical judgment and care are delivered solely by licensed healthcare professionals.

We deliver telehealth services (e.g., urgent care, therapy, psychiatry and, where covered, primary care) via secure audio/video and messaging. Where clinically appropriate, your provider may order labs, imaging, or other diagnostics performed by outside facilities and may rely on records you or your other providers share.

We also offer non-clinical wellness services by life-skills Coaches. Coaches are not licensed clinicians; they may collaborate with your healthcare professional as permitted.

This Notice describes how we use and disclose your Protected Health Information (“PHI”) and how you can exercise your rights regarding that information.

2. How is patient privacy protected?

We understand that information about you and your health is personal. By “health information,” we mean PHI as defined under federal law (HIPAA) and its implementing regulations, and as may be expanded or modified under applicable state laws. We use administrative, physical, and technical safeguards to protect your health information, and continuously update our practices to reflect evolving regulatory expectations and industry best practices — including cybersecurity enhancements, vendor oversight, access controls, audit logging, and risk-analysis practices. For example, the federal government has proposed and in some cases implemented changes to the HIPAA Security Rule to better address cybersecurity threats. We also comply with applicable state privacy laws (which may impose stricter requirements than federal law) and will honor those where applicable.

3. How do we use and disclose health information?

We may use and disclose your PHI for treatment, payment, and health-care operations. Under HIPAA, many of these uses and disclosures can be made without your explicit authorization. Substance Use Disorder (SUD) treatment records, which, consistent with the 2026 update to 42 CFR Part 2, may be used and disclosed for these TPO purposes only with your single, written consent.

A. Treatment

We may use and disclose your PHI to provide you with medical treatment and services. This includes coordinating your care among our Healthcare Professionals, Coaches (to the extent they are involved in care coordination), and other providers treating you. We may share your PHI with other professionals (e.g., labs, imaging centers, pharmacies) as necessary to carry out those treatment activities. This consent also covers the use and disclosure of your SUD treatment records for all treatment-related activities.

B. Payment

We may use and disclose your PHI to obtain payment from health plans or other third-party payors, to document the services and supplies provided, and to determine eligibility, cost estimates, prior-authorizations, or reimbursement. We may also share PHI to collect outstanding payments.

C. Health Care Operations

We may use and disclose your PHI for business management and general operations — for example, to review treatment and service performance, train staff, assess quality and outcomes, conduct business planning, audits, legal or regulatory compliance functions, and customer service. We may share PHI with Included Health, consultants, attorneys, vendors or others who perform functions on our behalf — provided they agree to safeguard the information.

D. Other permitted uses and disclosures

We may also use or disclose your PHI without your written authorization when required or permitted by law, including:

- To comply with federal, state or local laws, or with a court or administrative order.
- For public health and safety activities — e.g., reporting disease, medication or device adverse events, assisting in preventing or controlling injury, illness or disability.
- To respond to law enforcement requests, judicial orders, subpoenas or other legal processes.

- To coroners, medical examiners and funeral directors to identify a deceased person or determine cause of death.
- To facilitate organ or tissue donation or procurement.
- For health-research activities, consistent with regulatory requirements (including institutional review and safeguards).
- To avert or lessen a serious and imminent threat to the health or safety of you, the public or another person.
- For certain military and veterans' activities.
- For workers' compensation or employer-injury matters, as permitted or required under state law.
- To participate in health-information exchanges ("HIEs") in which we are a participant — for treatment, payment, health-care operations and other lawful purposes, as permitted by state law and HIE rules. Note: in some states you may be able to opt-in or opt-out of inclusion in an HIE; please contact us if you want to know whether that applies to you.

E. Marketing, Sale and Psychotherapy Notes

Unless you give us a separate written authorization, we will **not**:

- Use or disclose your PHI for marketing purposes (as defined under HIPAA).
- Sell your information.
- Disclose your psychotherapy notes. If state law affords greater protections, we will honour those additional rights.

F. How We Use Your Information to Improve Health Care (AI/Machine Learning)

We are committed to using new technologies to improve the quality, safety, and efficiency of your care. This includes using data to develop and train our Artificial Intelligence ("AI") and Machine Learning ("ML") tools.

- **For Better Care:** These tools help us analyze information, develop better clinical guidelines, improve diagnosis accuracy, and streamline our services, which are considered part of our Health Care Operations.

Using De-Identified Information

The most common way we use information for AI training is by making it anonymous.

- **What is it?** We remove all of the identifying details—like your name, address, dates, and account numbers—so the information can no longer be traced back to you. This is called de-identified information.
- **Our Use:** Once the information is de-identified, it is no longer covered by HIPAA privacy rules. We can use this anonymous data freely to train and improve our AI models without needing your specific permission.

Using Your PHI

If we need to use your PHI for AI training, we will only do so under the strictest privacy rules:

- **As Allowed by Law:** We can use PHI if it falls under Treatment, Payment, or our core Health Care Operations.
- **Your Permission is Needed:** For any AI training use that does *not* fall under these categories, we will ask for your specific written authorization first.
- **Privacy First:** Even when using PHI, we always follow the "minimum necessary" rule, meaning we only use the smallest amount of information required for the AI training project.

4. What are our responsibilities?

We are required by law to:

- Maintain the privacy of your PHI.
- Provide you with this Notice of our duties and privacy practices.
- Abide by the terms of this Notice currently in effect (unless we notify you of a revision).
- Notify you if there is a breach of unsecured PHI affecting you, in accordance with applicable federal and state law. We reserve the right to change the terms of this Notice, and to make the new terms effective for all PHI we maintain — including PHI created or received before the effective date of the revised Notice. Whenever we materially revise this Notice, we will post such revision on our site or otherwise make it available, and will notify you as required by law.
- As a Lawful Holder of Substance Use Disorder (SUD) treatment records received from Part 2 programs or other lawful holders, we are committed to protecting this information in accordance with 42 CFR Part 2 and the new HIPAA-aligned requirements. This includes complying with the HIPAA civil and criminal penalties for impermissible uses and disclosures of SUD records, effective February 16, 2026

5. Who will follow this Notice?

This Notice applies to:

- Any Healthcare Professional, Coach or other provider in the Doctor On Demand Professionals network authorized to access and/or enter information into your health record via our services;
- All departments and units of Doctor On Demand Professionals through which online health services are provided;
- All business associates, vendors, affiliates, and contractors of Doctor On Demand Professionals who handle PHI on our behalf — the obligations of such parties are reflected in our agreements with them and are incorporated herein by reference.

6. Your Rights Regarding Your Health Information

You have the following rights regarding your PHI (subject to any limitations under applicable federal or state law). In most cases you may exercise these rights by contacting our Corporate Compliance Officer (CCO) using the information in Section 10.

A. Access or copy

You have the right to obtain or inspect a copy of your PHI that we maintain, including an electronic copy where we maintain it electronically, and, where feasible, to have it transmitted to you or a third-party of your choice. We may deny your request under limited circumstances permitted by law. We may charge a reasonable, cost-based fee for copies, though state laws may limit or prohibit such fees.

B. Request amendment

If you believe your PHI is incorrect or incomplete, you may request an amendment. We may deny the request if we believe the PHI is accurate and complete or if certain conditions apply.

C. Accounting of disclosures

You may request an accounting of disclosures of your PHI we have made for the prior six (6) years (or longer if required under state law). This includes disclosures of your Substance Use Disorder (SUD) treatment records made for treatment, payment, and health-care operations, as required by the modernized 42 CFR Part 2 rules. This accounting does *not* include disclosures made after the date you requested the accounting.

D. Request restriction of uses and disclosures

You may request that we restrict how we use or disclose your PHI for treatment, payment or health-care operations. We are not required to agree to your request; if we do agree, we will comply except in emergency treatment situations.

If you request a restriction on disclosure of PHI to a health plan for payment or health-care operations and you pay out of pocket in full for such services, we will comply with your request where required by law.

E. Confidential communications

You may request that we communicate with you in a certain way or at a certain location (for example: a specific telephone number, email address or mailing address). We will accommodate reasonable requests.

F. Obtain a paper copy of this Notice

If you received this Notice electronically, you may request a paper copy at no cost.

G. Make choices about electronic health-information sharing

You may have additional rights under state law or under agreements by which we participate in health-information exchanges or other interoperability initiatives. For example, you may have the right in certain states to opt-in or opt-out of inclusion in an HIE, or the right to direct your electronic health record data to a personal health application of your choice. Under proposed HIPAA rule changes, patients may have expanded ability to direct ePHI to personal health apps.

7. Additional State Laws and Special Situations

Some state laws may impose additional protections on your health information (for example: reproductive health information, mental health information, substance use disorder records, genetic information, minors' records, or biometric data). Where state law gives you more rights than federal law, we will abide by the stronger standard. For example, under the final rule entitled "HIPAA Privacy Rule to Support Reproductive Health Care Privacy," certain disclosures of reproductive-health information to law-enforcement and other individuals are restricted.

8. Telehealth, Digital Communications and Interoperability

Because our services are delivered online, we use digital platforms, telehealth portals, mobile applications, and may exchange information electronically. In that context:

- We encrypt PHI in transit and at rest and require confidentiality and integrity of electronic health information.
- We conduct regular risk assessments and implement technical controls consistent with evolving standards (including proposed updates to the HIPAA Security Rule seeking to strengthen controls for ePHI).

- We may exchange electronic health information with other health-care organizations for treatment, payment, operations or as permitted by law — including through HIEs or interoperability frameworks.
- You may have rights to direct, access, or receive your health information through third-party personal health apps of your choice, consistent with interoperability requirements and applicable law.
- Because of the nature of telehealth, we remind you to maintain the security of your own device, internet connection and access credentials, and promptly inform us of any suspected unauthorized access or disclosure of your health information.

9. Breach Notification and Incident Response

If we discover a breach of unsecured PHI (or as otherwise defined by federal or state law) that affects you, we will notify you, the U.S. Department of Health and Human Services (HHS) and any other required agencies and individuals in accordance with the applicable law. We maintain a documented incident-response plan, conduct periodic testing, and include our business associates in breach-reporting obligations. Under the proposed HIPAA Security Rule revisions, business associates may be required to notify us within 24 hours of activation of their contingency plan.

10. How to Contact Us / Complaints

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of HHS. We will not retaliate or penalize you for filing a complaint with us or with the Secretary.

To contact us:

Chief Compliance and Privacy Officer (CCO)

Included Health, Inc.

1 California Street, Ste. 2300

San Francisco, CA 94111

Email: privacy@includedhealth.com

Phone: (855) 431-5533 (toll free)

If you are a registered user, you may also submit a message through the “chat” or member portal after logging in.

To file with the U.S. Department of Health and Human Services:

Secretary, U.S. Department of Health & Human Services, 200 Independence Avenue, S.W., Room 509 F, HHH, Washington, D.C. 20201; call 1-800-368-1019; or file online at

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

11. Versioning and Effective Date



Doctor On Demand Professionals - Notice of Privacy Practices

This Notice is effective as of the date listed above. We may change this Notice in the future. If we revise this Notice, the revised version will apply to all PHI we maintain — including PHI created or received prior to the revision. We will make the revised Notice available on our website and include a copy in our onboarding process or when requested.

Language Assistance Services: Notice of Availability

English: ATTENTION: If you speak English, language assistance services, free of charge, are available to you. Call 1-800-929-0926 (TTY: 711).

Español (Spanish): ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-800-929-0926 (TTY: 711).

繁體中文 (Chinese): 注意: 如果您使用繁體中文, 您可以免費獲得語言援助服務。請致電 1-800-929-0926 (TTY: 711)。

Tiếng Việt (Vietnamese): CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 1-800-929-0926 (TTY: 711).

한국어 (Korean): 주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 1-800-929-0926 (TTY: 711) 번으로 전화해 주십시오.

Tagalog (Tagalog – Filipino): PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa 1-800-929-0926 (TTY: 711).

Русский (Russian): ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 1-800-929-0926 (телетайп: 711).

ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم العربية (Arabic): 1-800-929-0926 (رقم هاتف الصم والبكم) 711).

Kreyòl Ayisyen (French Creole): ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 1-800-929-0926 (TTY: 711).

Français (French): ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 1-800-929-0926 (ATS : 711).

Polski (Polish): UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer 1-800-929-0926 (TTY: 711).

Português (Portuguese): ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para 1-800-929-0926 (TTY: 711).

Italiano (Italian): ATTENZIONE: In caso la lingua parlata sia l'italiano, sono disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero 1-800-929-0926 (TTY: 711).

Deutsch (German): ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: 1-800-929-0926 (TTY: 711).

日本語 (Japanese): 注意事項: 日本語を話される場合、無料の言語支援をご利用いただけます。1-800-929-0926 (TTY: 711) まで、お電話にてご連絡ください。

توجه: اگر به زبان فارسی گفتگو می کنید، تسهیلات زبانی بصورت رایگان برای شما فراهم می باشد. با فارسی (Farsi): 1-800-929-0926 (TTY: 711) تماس بگیرید.