



TeleHealthcare
Network

Augmenting Care Through Virtual Coverage

NOTICE OF PRIVACY PRACTICES

TELEHEALTHCARE NETWORK

**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.**

Effective Date: 1 January 2026

Date Adopted: 4 October 2026

This Notice applies to all protected health information created or maintained by
TeleHealthcare Network in connection with the care you receive.

If you have questions about this Notice, contact our Privacy Officer.

Contact information appears in Section 11.

1. About This Notice

TeleHealthcare Network ("TeleHCN," "we," "us," or "our") is required by law to protect the privacy of your health information, to give you this Notice explaining our legal duties and privacy practices, and to follow the terms of the Notice that is currently in effect.

"Protected health information," or PHI, means information about you — including demographic information — that could reasonably be used to identify you and that relates to your past, present, or future physical or mental health, the health care you receive, or the payment for that care.

TeleHCN provides physicians, nurse practitioners, and other clinicians who care for patients remotely, most often at rural and community hospitals. This means that a TeleHCN clinician may evaluate you, direct your treatment, order tests and medications, and document your care by secure video, telephone, and electronic medical record, without being physically present at your bedside. The privacy protections described in this Notice apply to that care exactly as they would to care delivered in person.

This Notice does not apply to information held by a hospital, clinic, laboratory, pharmacy, or health plan. Those organizations maintain their own records and issue their own notices. If you want to know how a hospital handles your information, ask that hospital for its Notice of Privacy Practices.

2. How We May Use and Share Your Health Information

The following categories describe the ways we are permitted to use and share your PHI without your written permission. Not every use is listed, but every use we make will fall into one of the categories below or into Section 3.

2.1 For Treatment

We use and share your health information to provide, coordinate, and manage your care.

Example: A TeleHCN hospitalist reviewing your chart overnight may discuss your condition with the bedside nurse, order labs and imaging, consult a cardiologist about your rhythm, adjust your medications, and give a handoff to the daytime team.

2.2 For Payment

We use and share your health information so that the care you receive can be billed and paid for by you, your insurer, or another payer.

Example: We may send information about the services provided to you, along with your diagnosis, to your health plan so that the plan will pay for the care, or to obtain prior authorization for a test or admission.

2.3 For Health Care Operations

We use and share your health information to run our organization and make sure the care we provide is safe and appropriate.

Example: We may review records to evaluate the quality of care our clinicians deliver, to conduct peer review and credentialing, to train and supervise clinicians, to investigate a complaint or adverse event, or to conduct internal audits and compliance monitoring.

2.4 With Business Associates

We contract with vendors who perform services for us — such as telehealth platform providers, electronic medical record and secure messaging vendors, billing companies, transcription services, IT and cloud hosting providers, attorneys, and accountants. We share only the information they need to do their work, and each is required by written agreement and by federal law to protect your information to the same standard we do.

2.5 With Hospitals and Other Providers

We share your information with the hospital or facility where you are being treated, and with other providers involved in your care, so that your treatment is coordinated and your record is complete.

2.6 With People Involved in Your Care

Unless you object, we may share information relevant to a person's involvement in your care — such as a spouse, family member, or friend who is helping with your treatment or payment. If you are not present or are unable to agree because of an emergency, we will use our professional judgment to decide whether sharing is in your best interest, and will share only what is directly relevant. We may also share information with a disaster relief organization so your family can be notified of your location and condition.

2.7 Appointment Reminders and Health Information

We may contact you to remind you of an appointment or follow-up, to tell you about treatment alternatives, or to describe health-related benefits and services that may be of interest to you.

3. Other Uses and Disclosures Permitted or Required by Law

We may use or share your health information without your permission in the following situations, subject to the conditions and limits set by law:

- **When required by law.** When a federal, state, or local law requires the disclosure.
- **Public health activities.** To prevent or control disease, injury, or disability; to report births and deaths; to report reactions to medications or problems with medical products; to notify people of recalls; and to notify a person who may have been exposed to a communicable disease.
- **Victims of abuse, neglect, or domestic violence.** To a government authority authorized to receive such reports, in accordance with law.
- **Health oversight activities.** To agencies that audit, investigate, license, inspect, or otherwise oversee the health care system and government benefit programs.
- **Judicial and administrative proceedings.** In response to a court or administrative order, and in response to a subpoena, discovery request, or other lawful process where the required assurances about notice to you or a protective order have been provided.
- **Law enforcement.** To identify or locate a suspect, fugitive, material witness, or missing person; about a crime victim under limited conditions; about a death we believe may have resulted from criminal conduct; about criminal conduct on our premises; and in an emergency to report a crime.
- **Coroners, medical examiners, and funeral directors.** To identify a deceased person, determine cause of death, or allow them to carry out their duties.
- **Organ and tissue donation.** To organizations that handle organ, eye, or tissue procurement, banking, or transplantation.

- **Research.** For research that has been approved by an institutional review board or privacy board that has reviewed the research proposal and established protocols to protect your privacy.
- **To avert a serious threat to health or safety.** When necessary to prevent or lessen a serious and imminent threat to you or to the health or safety of another person or the public, to someone able to help prevent the threat.
- **Specialized government functions.** For military and veterans activities, national security and intelligence activities, protective services for the President and others, correctional institutions and law enforcement custody, and eligibility for certain government benefit programs.
- **Workers' compensation.** As authorized by and to the extent necessary to comply with workers' compensation and similar programs.

4. Uses and Disclosures That Require Your Written Authorization

The following uses and disclosures will be made only with your written authorization:

- **Psychotherapy notes,** except in the limited circumstances the law permits (for example, for our own training programs or to defend ourselves in a legal action you bring).
- **Marketing.** Most uses and disclosures of your information for marketing purposes.
- **Sale of your information.** We do not and will not sell your health information.
- **Fundraising.** We do not conduct fundraising. If that ever changes, you will have the right to opt out of fundraising communications.

Any other use or disclosure not described in this Notice will be made only with your written authorization. You may revoke an authorization at any time, in writing, by contacting our Privacy Officer. A revocation stops future uses and disclosures but does not undo anything we already did in reliance on your authorization.

Recording of Telehealth Encounters

TeleHCN does not video- or audio-record clinical encounters as a routine practice. If a recording is ever proposed for a purpose other than treatment documentation, we will obtain your written authorization first. You may decline a recording without affecting the care you receive.

5. Your Rights Regarding Your Health Information

You have the following rights. To exercise any of them, submit a written request to our Privacy Officer using the contact information in Section 11. We will respond within the timeframes required by law.

5.1 Right to Inspect and Get a Copy

You have the right to inspect and obtain a copy of the health information we maintain about you in a designated record set, including in an electronic format if we maintain it electronically. We will act on your request within 30 days, with one 30-day extension if we notify you of the reason for the delay. We may charge a reasonable, cost-based fee for copying, mailing, or supplies. In limited circumstances we may deny a request, and certain denials are subject to review by a licensed health care professional who was not involved in the original decision.

5.2 Right to Request an Amendment

If you believe information we hold about you is incorrect or incomplete, you may ask us to amend it. Your request must be in writing and must explain why the amendment is warranted. We may deny the request if the information was not created by us, is not part of the designated record set, is not available for inspection, or is accurate and complete. If we deny your request, we will tell you why in writing, and you may submit a statement of disagreement that will be included with the record.

5.3 Right to an Accounting of Disclosures

You have the right to request a list of certain disclosures we have made of your health information in the six years before the date of your request. The list does not include disclosures made for treatment, payment, or health care operations, disclosures made to you, disclosures you authorized, and certain other disclosures the law excludes. The first accounting in any 12-month period is free; we may charge a reasonable, cost-based fee for additional requests, and we will tell you the cost in advance so you may withdraw or modify your request.

5.4 Right to Request Restrictions

You have the right to ask us to restrict how we use or share your information for treatment, payment, or health care operations, or with someone involved in your care. We are not required to agree to most restriction requests, and if we do agree we will follow the restriction except in an emergency.

One restriction we must honor: if you pay in full, out of pocket, for a specific item or service, and the disclosure is to a health plan for payment or health care operations purposes and is not otherwise required by law, we must not disclose that information to your health plan.

5.5 Right to Confidential Communications

You have the right to ask us to communicate with you about medical matters in a certain way or at a certain location — for example, by calling a mobile number rather than a home number, or by sending mail to an alternate address. We will accommodate reasonable requests and will not ask you to explain the reason for the request.

5.6 Right to a Paper Copy of This Notice

You have the right to a paper copy of this Notice at any time, even if you agreed to receive it electronically. Ask our Privacy Officer and we will provide one.

5.7 Right to Be Notified of a Breach

You have the right to be notified if we discover a breach of your unsecured protected health information. We will notify you without unreasonable delay and no later than the deadline set by law.

5.8 Right to Choose Someone to Act for You

If you have given someone a medical power of attorney, or if someone is your legal guardian, that person can exercise these rights and make choices about your health information. We will verify that the person has the authority to act for you before we take any action.

6. Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.

- We will notify you promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this Notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we may, in writing. If you tell us we may and then change your mind, you may revoke that permission in writing at any time.
- We limit our uses, disclosures, and requests for your information to the minimum necessary to accomplish the purpose, except for disclosures for treatment, disclosures to you, and certain other disclosures the law excludes from this requirement.
- We train our workforce and contracted clinicians on privacy and security, and we impose sanctions on anyone who violates our policies or the law.

7. How We Protect Your Information in a Telehealth Setting

Because our clinicians work remotely, we apply specific safeguards to the technology used to deliver your care:

- Clinical video, messaging, and record access occur only on encrypted platforms approved by TeleHCN and covered by written agreements requiring HIPAA compliance.
- Clinicians conduct encounters from private, secure locations where conversations cannot be overheard, and use privacy screens where appropriate.
- Access to your record requires individual, uniquely identifiable credentials with multi-factor authentication. Credentials are never shared, so every access can be traced to one person.
- Access to records is logged and audited. Looking at a record without a treatment, payment, or operations reason is a terminable offense at TeleHCN.
- Personal text messaging, personal email, and consumer messaging applications are prohibited for any communication containing your health information.
- Your health information is never entered into consumer artificial intelligence tools or unapproved cloud services.
- Devices used to access your information are encrypted, and lost or stolen devices must be reported immediately so access can be revoked.

No method of electronic transmission or storage is perfectly secure. If a safeguard fails, our obligation to notify you under Section 5.7 applies.

8. Information With Special Protections

Some categories of health information are subject to stricter rules under federal or state law than the rules described above. Depending on where you receive care, these may include records of substance use disorder treatment protected by 42 C.F.R. Part 2, mental health and psychotherapy records, HIV and other communicable disease test results, genetic information, and reproductive health information. Where a stricter law applies, we follow the stricter law. In many cases this means we cannot share that information without your specific written permission, even for treatment.

The law of the state where you are located when you receive care may give you privacy rights beyond those described in this Notice. Where state law is more protective of your privacy than HIPAA, we follow state law.

9. Changes to This Notice

We reserve the right to change this Notice and to make the revised Notice effective for health information we already have about you as well as any information we receive in the future. The Notice currently in effect will be posted on our website at telehealthcarenetwork.com, and the effective date appears on the first page. You may obtain a copy of the current Notice at any time by contacting our Privacy Officer. If we make a material change, we will post the revised Notice promptly and make it available on request.

10. How to File a Complaint

If you believe your privacy rights have been violated, you may file a complaint with us, with the federal government, or both.

10.1 Complaint to TeleHCN

Submit your complaint in writing to our Privacy Officer at the address in Section 11. Describe what happened and when, as specifically as you can. We will investigate and respond.

10.2 Complaint to the Federal Government

You may file a complaint with the Secretary of the U.S. Department of Health and Human Services, Office for Civil Rights. Complaints must generally be filed within 180 days of when you knew or should have known of the violation.

- Online: www.hhs.gov/ocr/privacy/hipaa/complaints/
- Mail: Office for Civil Rights, U.S. Department of Health and Human Services, 200 Independence Avenue SW, Room 509F, HHH Building, Washington, D.C. 20201
- Phone: 1-877-696-6775

You Will Not Be Penalized

We will not retaliate against you, deny you care, or change how you are treated in any way because you filed a complaint or exercised any right described in this Notice.

11. Who to Contact

For questions about this Notice, to exercise any of your rights, or to file a complaint, contact:

TeleHealthcare Network — Privacy Officer

Vimarsh Raina, MD — Privacy Officer

Telephone: 715-321-4122

Email: dr.raina@telehealthcarenetwork.com

Mailing Address: TeleHealthcare Network LLC, 929C Seneca Rd, Great Falls, VA 22066

Website: telehealthcarenetwork.com

Effective Date of This Notice: 1 January 2026

This Notice supersedes all previous Notices of Privacy Practices issued by TeleHealthcare Network.



TeleHealthcare
Network
Augmenting Care Through Virtual Coverage

ACKNOWLEDGMENT OF RECEIPT

TeleHealthcare Network Notice of Privacy Practices

I acknowledge that I have been provided with a copy of the TeleHealthcare Network Notice of Privacy Practices, which describes how my health information may be used and shared and how I can access that information.

I understand that:

- I may request a paper copy of the Notice at any time, free of charge.
- The current version of the Notice is available at telehealthcarenetwork.com.
- TeleHealthcare Network may change the Notice, and the revised Notice will apply to health information it already holds about me.
- Signing this form does not waive any of my privacy rights and does not authorize any use or disclosure of my information beyond what the Notice and the law permit.

Printed Name of Patient

Date of Birth

Signature of Patient or Personal Representative

Date

If signed by a Personal Representative, relationship / authority

Date of Service

For Office Use Only

Good faith effort was made to obtain written acknowledgment of receipt, but acknowledgment could not be obtained because:

- Patient refused to sign
- Patient was unable to sign due to emergency or incapacity
- Encounter was conducted remotely and signature could not be obtained
- Other: _____

Staff Name and Title

Date