



NOTICE OF PRIVACY PRACTICES

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.

If you have any questions about this Notice, please contact our Privacy Officer at 970.728.3848

This Notice of Privacy Practices describes how Telluride Regional Medical Center may use and disclose your protected health information to carry out treatment, payment or health care operations and for the purposes that are permitted or required by law. It also describes your rights to access and control your protected health information. "Protected Health Information" is information about you, including demographic information, that may identify you and that relates to your past, present, or future physical or mental health or condition and related health care services. We are required to abide by the terms of this Notice of Privacy Practices. We may change the terms of our notice at any time. The new notice will be effective for all protected health information that we maintain at that time. Upon your request, we will provide you with any revised Notice of Privacy Practices by accessing, calling the office and requesting that a revised copy be sent to you in the mail or asking for one at the time of your next appointment.

SUBSTANCE USE DISORDER TREATMENT

Some of our patients receive services related to substance use disorders (SUD). Certain records from those services are protected by a federal confidentiality law called "Part 2." These protections are in addition to HIPAA.

We protect your SUD treatment records under 42 C.F.R. Part 2, HIPAA, and Colorado law (C.R.S. 27-81-113), which strictly limits use or disclosure of these records and privileges them to the patient.

1. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Your protected health information may be used and disclosed by your provider, our office staff and others outside of our office that are involved in your care and treatment for the purpose of providing health care services to you. Following are examples of the types of uses and disclosures of your protected health care information that the provider's office is permitted to make. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures that may be made by our office.

Treatment: We will use and disclose your protected health information to provide, coordinate, or manage your health care and any related services. This includes the coordination or management of

your health care with a third party that has already obtained your permission to have access to your protected health information. For example, we would disclose your protected health information, as necessary, to a home health agency that provides care to you. We will also disclose protected health information to other providers who may be treating you.

For example, your protected health information may be provided to a provider to whom you have been referred to ensure that the provider has the necessary information to diagnose or treat you. In addition, we may disclose your protected health information from time-to-time to another provider or health care provider (e.g., a specialist or laboratory) who, at the request of your provider, becomes involved in your care by providing assistance with your health care diagnosis or treatment to your provider.

Payment: Your protected health information will be used, as needed, to obtain payment for your health care services. This may include certain activities that your health insurance plan may undertake before it approves or pays for the health care services we recommend for you, such as: making a determination of eligibility or coverage for insurance benefits, reviewing services provided to you for medical necessity, and undertaking utilization review activities.

For example, obtaining approval for a hospital stay may require that your relevant protected health information be disclosed to the health plan to obtain approval for the hospital admission.

Healthcare Operations: We may use or disclose, as needed, your protected health information in order to support the business activities of Telluride Hospital District's practice. These activities include, but are not limited to, quality assessment activities, employee review activities, training of medical students, licensing, marketing and fundraising activities, and conducting or arranging for other business activities.

For example, we may disclose your protected health information to medical school students that see patients at our office. In addition, we may use a sign-in sheet at the registration desk where you will be asked to sign your name and indicate your provider. We may also call you by name in the waiting room when your provider is ready to see you. We may use or disclose your protected health information, as necessary, to contact you to remind you of your appointment. We will share your protected health information with third party "business associates" that perform various activities (e.g., billing, transcription services) for the practices.

Whenever an arrangement between our office and a business associate involves the use or disclosure of your protected health information, we will have a written contract that contains terms that will protect the privacy of your protected health information. We may use or disclose your protected health information, as necessary, to provide you with information about treatment alternatives or other health-related benefits and services that may be of interest to you. We may also use and disclose your protected health information for other marketing activities.

For example, your name and address may be used to send you a newsletter about our practice and the services we offer. We may also send you information about products or services that we believe may be beneficial to you. We may use or disclose your demographic information, as necessary, in order to contact you for fundraising activities supported by our office. If you do not want to receive

these materials, please contact our Privacy Officer and request that these materials not be sent to you.

Health Information Exchange: Our organization uses the Quality Health Network (“QHN”) health information exchange system (“HIE”) for the secure exchange of electronic health information between authorized medical providers. The HIE protects patient privacy by using various security features that include encryption, password protection and information access and audit controls.

In some cases, you may limit a medical providers’ ability to view your health information through use of the HIE. This right is referred to as “Opt-Out”. If you choose to Opt-Out a medical provider who you are seeing for care, will NOT be able to view your health information via an HIE query, EVEN IN AN EMERGENCY. Opting Out can inhibit access to critical information that may help your medical providers manage your care and may increase duplication and costs. However, your medical provider(s) may continue to use the HIE to electronically direct the exchange of your health information, such as diagnostic test results.

To Opt-Out, you must complete a written request with your medical provider. If you want more information about the HIE or to discuss Opt-Out, please contact us at (970)-728-3848.

Substance Use Disorder Treatment Information: We will protect SUD treatment records in accordance with 42 C.F.R. Part 2 and HIPAA. We will provide this notice, follow it, and promptly update it if our practices change in a material way. We will not use or disclose SUD records unless allowed by Part 2 and HIPAA, or unless you give us written permission (consent) as described below.

Uses and Disclosures of Protected Health Information Based upon your Written Authorization: Other uses and disclosures of your protected health information will be made only with your written authorization, unless otherwise permitted or required by law as described below. You may revoke this authorization, at any time, in writing, except that your provider or the provider’s practice has taken an action in reliance on the use or disclosure indicated in the authorization.

We may use and disclose your protected health information in the following instances. You have the opportunity to agree or object to the use or disclosure of all or part of your protected health information. If you are not present or able to agree or object to the use or disclosure of the protected health information, then your provider may, using professional judgment, determine whether the disclosure is in your best interest. In this case, only the protected health information that is relevant to your health care will be disclosed.

Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your protected health information that is directly related to the person’s involvement in your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose protected health information to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location, general condition, or death. Finally, we may use or disclose your protected health information to an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other individuals involved in your health care.

SUD Treatment: You may sign one consent to authorize ongoing use and disclosure of your SUD records for treatment, payment, and healthcare operations. You can revoke it anytime in writing, except for disclosures already made. Covered entities receiving these records under your consent may redisclose them under HIPAA, except for legal proceedings against you without your further permission.

Other Permitted and Required Uses and Disclosures That May Be Made Without Your Authorization or Opportunity to Object: We may use or disclose your protected health information in the following situations without your authorization. The situations include:

Required By Law: We may use or disclose your protected health information to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, as required by law, of any such use or disclosures.

Public Health: We may disclose your protected health information for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. The disclosure will be made for the purpose of controlling disease, injury, or disability. We may also disclose your protected health information, if directed by the public health authority, to a foreign government agency that is collaborating with the public health authority.

Communicable Disease: We may disclose your protected health information, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

Health Oversight: We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil right laws.

Abuse or Neglect: We may disclose your protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your protected health information if we believe that you have been a victim of abuse, neglect, or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Food and Drug Administration: We may disclose your protected health information to a person or company required by the Food and Drug Administration to report adverse events, product defects or problems, biologic product deviations, track products; to enable product recalls; to make repairs or replacements, or to conduct post-marketing surveillance, as required.

Legal Proceedings: We may disclose protected health information in the course of any judicial or administrative proceedings, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), in certain conditions in response to a subpoena, discovery request or other lawful process.

Law Enforcement: We may also disclose protected health information, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1)

legal processes and other releases required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of the practice, and (6) medical emergency (not on the Practice's premises) and it is likely that a crime has occurred.

Coroners, Funeral Directors, and Organ Donation: We may disclose protected health information to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose protected health to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We may disclose such information in reasonable anticipation of death. Protected health information may be used and disclosed for cadaver organ, eye, or tissue donation purposes.

Research: We may disclose your protected health information to researchers when their research has been approved by an institutional review board (IRB) that has reviewed the research proposal and established protocols to ensure the privacy of your protected health information.

Criminal Activity: Consistent with applicable federal and state laws, we may disclose your protected health information, if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose protected health information if necessary for law enforcement authorities to identify or apprehend an individual.

Military Activity and National Security: When the appropriate conditions apply, we may use or disclose protected health information of individuals who are Armed Forces personnel (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veteran Affairs of your eligibility for benefits, or (3) to foreign military authority if you are member of that foreign military services. We may also disclose your protected health information to authorized federal officials for conduction of national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

Workers' Compensation: Your protected health information may be disclosed by us as authorized to comply with workers' compensation laws and other similar legally-established programs.

Inmates: We may use or disclose your protected health information if you are an inmate of a correctional facility and your provider created or received your protected health information in the course of providing care to you.

Required Uses and Disclosures: Under the law, we must make disclosures to you and when required by the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the requirements of Section 164.500 et. Seq.

SUD Treatment Disclosures: We may disclose SUD treatment information without your consent when legally permitted, always following both Part 2 and HIPAA rules. This may include for the purpose of: medical emergencies, court orders (for child abuse, cause of death), specific public health purposes, or research purposes.

2. YOUR RIGHTS

Following is a statement of your rights with respect to your protected health information and a brief description of how you may exercise these rights.

You have the right to inspect and copy your protected health information. This means you may inspect and obtain a copy of protected health information about you that is contained in a designated record set for as long as we maintain the protected health information. A “designated record set” contains medical and billing records and any other records that your provider and the practice use for making decisions about you. Under Colorado State Law, the records encompassed include x-ray and other films, which are subject to distinct rules. [Colo. Rev. Stat. Ann. 25-1-801.] Medical information transmitted during the delivery of health care via telemedicine is part of the patient’s medical record maintained by the facility.

An exception to access is made for records pertaining to mental health problems or notes by a provider that, in the opinion of a licensed provider who practices psychiatry and is an independent third party, would have significant negative psychological impact. With regards to these records, a summary pertaining to the patient’s mental health problems may be made available following termination of the treatment program.

Additionally, under federal law, however, you may not inspect or copy the following records: information compiled in reasonable anticipation of or use in a civil, criminal, or administrative action or proceeding, and protected health information that is subject to law that prohibits access to protected health information.

With respect to a minor who has consented to the diagnosis or treatment of venereal disease or addiction to or use of drugs without parental consent, the health care facility may not release the related medical records of the minor to a parent, guardian, or any person other than the minor or his designated representative. [Colo. Rev. Stat. Ann. 25-1-801(1)(d)]

Depending on the circumstances, you may have a right to have a decision to deny access reviewed. Please contact our Privacy Officer if you have questions about access to your medical record.

You have the right to request a restriction of your protected health information. This means you may ask us not to use or disclose any part of your protected health information for the purposes of treatment, payment, or healthcare operations. You may also request that any part of your protected health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. Your request must state the specific restriction requested and to whom you want the restriction to apply. Your provider is not required to agree to a restriction that you may request. If the provider believes it is in your best interest to permit use and disclosure of your protected health information, your protected health information will not be restricted. If your provider does agree to the requested restriction, we may not use or disclose your protected health information in violation of that restriction unless it is needed to provide emergency treatment. With this in mind, please discuss any restriction you wish to request with your provider.

You have the right to request to receive confidential communications from us by alternative means or at an alternative location. We will accommodate reasonable requests. We may also condition this accommodation by asking you for information as to how payment will be handled or specify an alternative address or other method of contact. We will not request an explanation from you as to the basis for the request. Please make this request in writing to our Privacy Officer.

You may have the right to have your provider amend your protected health information. This means you may request an amendment of protected health information about you in a designated record set for as long as we maintain this information. In certain cases, we may deny your request for an amendment. If we deny your request for amendment, you have the right to file a statement of disagreement with us and we may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal. Please contact our Privacy Officer if you have questions about amending your medical record.

You have the right to receive an accounting of certain disclosures we have made, if any, of your protected health information. This right applies to disclosures for purposes other than treatment, payment, or healthcare operations as described in this Notice of Privacy Practices. It excludes disclosures we may have made to you, to family members or friends involved in your care, or for notification purposes. You have the right to receive specific information regarding these disclosures that occurred after April 14, 2003. The right to receive this information is subject to certain exceptions, restrictions, and limitations.

All SUD disclosures authorized by you will include: "42 CFR Part 2 prohibits unauthorized use or disclosure of these records."

Anti-Discrimination & Confidentiality: We will not use your SUD records to discriminate against you in housing, employment, or services. Under Colorado law and federal rules, these records remain privileged and confidential.

You have the right to obtain a paper copy of this notice from us, upon request, even if you have agreed to accept this notice electronically.

3. COMPLAINTS

You may complain to us or the secretary of health and human services if you believe your privacy rights have been violated by us. You may file a complaint with us by notifying our Privacy Officer of your complaint. We will not retaliate against you for filing a complaint.

You may contact our Privacy Officer at 970.728.3848 for further information about the complaint process.

This notice was published and becomes effective on April 14, 2003. Last updated by current HIPAA Privacy Officer: February 10, 2026.