Colorado Dermatology Institute

Regulations

By signing the Informed Consent Signature Page, you are indicating you understand each of these Regulations and the role that CDI and the patient play in each Regulation.

Patient Privacy and Protected Health Information (HIPAA) *Revised May 2016*

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 the Privacy Officer at 8580 Scarborough Dr., Suite 225, Colorado Springs, CO 80920.

OUR OBLIGATIONS:

We are required by law to:

- Maintain the privacy of Protected Health Information (PHI) (information that identifies you or your dermatologic condition(s))
- Give you this notice of our legal duties and privacy practices regarding PHI about you
- Follow the terms of our notice that is currently in effect

HOW WE MAY USE AND DISCLOSE PHI:

The following describes the ways we may use and disclose PHI that identifies you and the health condition(s) for which you are being treated. **Except for the purposes described below, we will use and disclose PHI only with your written permission.** You may revoke such permission at any time by writing to the Privacy Officer at 8580 Scarborough Dr., Suite 225, Colorado Springs, CO 80920.

Your PHI may be used and disclosed by your physician, our office staff and others outside of our offices who are involved in your care and treatment for the purpose of providing health care services to you. Your PHI may also be used and disclosed to pay your health care bills and to support the operation of your physician's practice.

Following are examples of the types of uses and disclosures of your PHI that your physician'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.

For Treatment. We may use and disclose PHI for your treatment and to provide you with treatment-related health care services. For example, we may disclose PHI to doctors, nurses, technicians, or other personnel, including people outside our office, who are involved in your medical care and need the information to provide you with medical care.

For Payment. We may use and disclose PHI so that we or others may bill and receive payment from you, an insurance company or a third party for the treatment and services you received. For example, we may give information about you to your health plan so that they will pay for your treatment.

Health Care Operations. We may use or disclose, as needed, your PHI in order to support the business activities of your physician's practice. These activities include, but are not limited to, quality assessment

activities, employee review activities, training of medical students, licensing, fundraising activities, and conducting or arranging for other business activities.

We will share your PHI with third party "business associates" that perform various activities (for example, billing or transcription services) for our practice. Whenever an arrangement between our office and a business associate involves the use or disclosure of your PHI, we will have a written contract that contains terms that will protect the privacy of your PHI.

We may use or disclose your PHI, as necessary, to provide you with information about treatment alternatives or other health-related benefits and services that may be of interest to you. You may contact our Privacy Officer at 8580 Scarborough Dr., Suite 225, Colorado Springs, CO 80920 to request that these materials not be sent to you.

Appointment Reminders, Treatment Alternatives and Health Related Benefits and Services. We may use and disclose PHI such as your name, address or phone number to contact you to remind you that you have an appointment with us. We also may use and disclose PHI (name, address, phone number) to tell you about treatment alternatives or health-related benefits and services that may be of interest to you.

Individuals Involved in Your Care or Payment for Your Care. When appropriate, we may share PHI with a person who is involved in your medical care or payment for your care, such as your family or a legal representative/guardian.

Research. Under certain circumstances, we may use and disclose PHI for research. For example, a research project may involve comparing the health of patients who received one treatment to those who received another for the same condition. Before we use or disclose PHI for research, the project will go through a special approval process. Even without special approval, we may permit researchers to look at records which have been stripped of identifying PHI to help them select a patient's file that may be included in their research project or for other similar purposes, as long as they do not have access to the patient's identifying information unless we have obtained written permission from the patient to release that identifying PHI.

SPECIAL SITUATIONS:

Required By Law: We may use or disclose your PHI 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, if required by law, of any such uses or disclosures.

Public Health: We may disclose your PHI for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. For example, a disclosure may be made for the purpose of preventing or controlling disease, injury or disability.

Health Oversight: We may disclose PHI 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 rights laws.

Abuse or Neglect: We may disclose your PHI to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your PHI 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.

Colorado Dermatology Institute

Food and Drug Administration. We may disclose your PHI to a person or company required by the Food and Drug Administration for the purpose of quality, safety, or effectiveness of FDA-regulated products or activities including, to report adverse events, product defects or problems, biologic product deviations, to

track products; to enable product recalls; to make repairs or replacements, or to conduct post marketing surveillance, as required.

Business Associates. We may disclose PHI to our business associates that perform functions on our behalf or provide us with services if the information is necessary for such functions or services. For example, we may use a dermatopathology laboratory to assist us in the diagnosis of your dermatologic condition(s). All of our business associates are obligated to protect the privacy of your PHI and are not allowed to use or disclose any information other than as specified in our contract.

Military Activity and National Security. When the appropriate conditions apply, we may use or disclose PHI 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 Veterans Affairs of your eligibility for benefits, or (3) to foreign military authority if you are a member of that foreign military services. We may also disclose your PHI to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

Workers' Compensation. We may release PHI for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Data Breach Notification Purposes. We may use or disclose your PHI to provide legally required notices of unauthorized access to or disclosure of your PHI.

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

Law Enforcement. We may release PHI if asked by a law enforcement official if the information is: (1) in response to a court order, subpoena, warrant, summons or similar process; (2) limited information to identify or locate a suspect, fugitive, material witness, or missing person; (3) about the victim of a crime even if, under certain very limited circumstances, we are unable to obtain the person's agreement; (4) about a death we believe may be the result of criminal conduct; (5) about criminal conduct on our premises; and (6) in an emergency to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.

Coroners, Medical Examiners, Organ and Tissue Donation, and Funeral Directors. We may release PHI to a coroner, medical examiner, those involved in Organ harvesting or transport, and to Funeral Directors as necessary for them to perform their legal functions.

Inmates or Individuals in Custody. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release PHI to the correctional institution or law enforcement official. This release would be if necessary: (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) the safety and security of the correctional institution.

Uses and Disclosures of PHI Based upon Your Written Authorization. Other uses and disclosures of your PHI will be made only with your written authorization, unless otherwise permitted or required by law as described below. You may revoke this authorization in writing at any time. If you revoke your authorization,

we will no longer use or disclose your PHI for the reasons covered by your written authorization. Please understand that we are unable to take back any disclosures already made with your authorization.

Other Permitted and Required Uses and Disclosures That Require Providing You the Opportunity to Agree or Object. We may use and disclose your PHI in the following instances. You have the opportunity to agree or object to the use or disclosure of all or part of your PHI. If you are not present or able to agree or object to the use or disclosure of the PHI, then your physician may, using professional judgment, determine whether the disclosure is in your best interest.

Individuals Involved in Your Care or Payment for Your Care. Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your PHI that directly relates to that 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.

Disaster Relief. We may disclose your PHI to disaster relief organizations that seek your PHI to coordinate your care, or notify family and friends of your location or condition in a disaster. We will provide you with an opportunity to agree or object to such a disclosure whenever we practically can do so.

YOUR WRITTEN AUTHORIZATION IS REQUIRED FOR OTHER USES AND DISCLOSURES:

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

1. Uses and disclosures of PHI for marketing purposes; and
2. Disclosures that constitute a sale of your PHI

Other uses and disclosures of PHI not covered by this Notice or the laws that apply to us will be made only with your written authorization. If you do give us an authorization, you may revoke it at any time by submitting a written revocation to our Privacy Officer and we will no longer disclose PHI under the authorization. But disclosure that we made based on your authorization before you revoked it will not be affected by the revocation.

YOUR RIGHTS:

You have the following rights regarding PHI we have about you:

Right to Inspect and Copy. You have a right to inspect and copy PHI that may be used to make decisions about your care or payment for your care. This includes medical and billing records, other than psychotherapy notes. To inspect and copy this PHI, you must make your request, in writing, to the Colorado Dermatology Institute Privacy Officer at 8580 Scarborough Dr, Suite 225, Colorado Springs, CO 80920. We have up to 30 days to make your PHI available to you and we may charge you a reasonable fee for the costs of copying, mailing or other supplies associated with your request.

Under federal law, however, you may not inspect or copy the following records: psychotherapy notes; information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; and laboratory results that are subject to law that prohibits access to PHI. Depending on the circumstances, a decision to deny access may be reviewable. In some circumstances, you may have a right to have this decision reviewed. Please contact the Privacy Officer at 8580 Scarborough Dr, Suite 225, Colorado Springs, CO 80920 if you have questions about access to your medical record.

Right to an Electronic Copy of Electronic Medical Records. Your PHI is maintained in an electronic format (known as an electronic medical record or an electronic health record). You have the right to request that an

electronic copy of your record be given to you or transmitted to another individual or entity. We will make every effort to provide access to your PHI in the form or format you request, if it is readily producible in such form or format. If the PHI is not readily producible in the form or format you request,

your record will be provided in either our standard electronic format or if you do not want this form or format, a readable hard copy form. We may charge you a reasonable, cost-based fee for the labor associated with transmitting the electronic medical record.

Right to Get Notice of a Breach. You have the right to be notified upon a breach of any of your unsecured PHI.

Right to Amend. If you feel that PHI we have is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for our office. To request an amendment, you must make your request, in writing, to the Privacy Officer at 8580 Scarborough Dr., Suite 225, Colorado Springs, CO 80920.

Right to an Accounting of Disclosures. You have the right to request a list of certain disclosures we made of PHI for purposes other than treatment, payment and health care operations or for which you provided written authorization. To request an accounting of disclosures, you must make your request, in writing, to the Privacy Officer at 8580 Scarborough Dr., Suite 225, Colorado Springs, CO 80920.

Right to Request Restrictions. You have the right to request a restriction or limitation on the PHI we use or disclose for treatment, payment, or health care operations. You also have the right to request a limit on the PHI we disclose to someone involved in your care or the payment for your care. For example, you could ask that we not share information about a particular diagnosis or treatment with your spouse. To request a restriction, you must make your request, in writing, to the Privacy Officer at 8580 Scarborough Dr., Suite 225, Colorado Springs, CO 80920.

We are not required to agree to your request unless you are/were a “self pay” patient asking us to restrict the use and disclosure of your PHI to a health plan for payment or health care operation purposes and such information you wish to restrict pertains solely to a health care item or service for which you have paid us “out-of-pocket” in full. If we agree, we will comply with your request unless the information is needed to provide you with emergency treatment.

Self Pay/Out-of-Pocket-Payments. If you paid out-of-pocket (or in other words, you have requested that we not bill your health plan) in full for a specific item or service, you have the right to ask that your PHI with respect to that item or service not be disclosed to a health plan for purposes of payment or health care operations, and we will honor that request.

Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you by mail or at work. To request confidential communications, you must make your request, in writing, to the Privacy Officer at 8580 Scarborough Dr., Suite 225, Colorado Springs, CO 80920. Your request must specify how or where you wish to be contacted. We will accommodate reasonable requests.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice. You may obtain a copy of this notice at our web site, www.coderm.com. To obtain a paper copy of this notice, write the Privacy Officer at 8580 Scarborough Dr., Suite 225, Colorado Springs, CO 80920.

Colorado Dermatology Institute

Changes to this Notice. We reserve the right to change this notice and make the new notice apply to PHI we already have as well as any information we receive in the future. We will post a copy of our current notice at our office. The notice will contain the effective date on the first page, in the top right-hand corner.

Complaints. If you believe your privacy rights have been violated, you may file a complaint with our office or with the Secretary of the Department of Health and Human Services. All complaints must be made in writing. To file a complaint with our office, contact the Privacy Officer at 8580 Scarborough Dr., Suite 225, Colorado Springs, CO 80920. **You will not be penalized for filing a complaint.**

Identity Theft Prevention and Detection and Red Flag Rule Compliance Policy *Revised May 2016*

It is the policy of Colorado Dermatology Institute, CDI, to follow all federal and state laws and reporting requirements regarding identity theft. Specifically, this policy outlines how CDI will (1) identify, (2) detect and (3) respond to "red flags." A "red flag" as defined by this policy includes a pattern, practice, or specific account or record activity that indicates possible identity theft.

Procedures:

Identify Red Flags

In the course of caring for patients, CDI may encounter inconsistent or suspicious documents, information or activity that may signal identity theft. CDI identifies the following as potential red flags, and this policy includes procedures describing how to detect and respond to these red flags below:

1. A complaint or question from a patient based on the patient's receipt of:
   - A bill for another individual
   - A bill for a product or service that the patient denies receiving
   - A bill from a health care provider that the patient never patronized
   - A notice of insurance benefits (or explanation of benefits) for health care services never received
2. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.
3. A complaint or question from a patient about the receipt of a collection notice from a bill collector.
4. A patient or health insurer report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.
5. A complaint or question from a patient about information added to a credit report by a health care provider or health insurer.
6. A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
7. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
8. A notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency, including but not limited to a Medicare or Medicaid fraud agency.

Detect Red Flags

CDI practice staff will be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud. CDI will verify patient identity, address and insurance coverage at the time of patient registration/check-in.

Procedures:

1. When a patient calls to request an appointment, the patient will be asked to bring the following at the time of the appointment:

- Driver's license or other state issued photo ID
- Current health insurance card
- Utility bills or other correspondence showing current residence if the photo ID does not show the patient's current address. If the patient is a minor, the patient's parent or guardian should bring the information listed above.

2. When the patient arrives for the appointment, the patient will be asked to produce the information listed above. This requirement may be waived for patients who have visited the practice within the last six months.
3. If the patient has not completed the registration form within the last six months, registration staff will verify current information on file and, if appropriate, update the information.
4. Staff should be alert for the possibility of identity theft in the following situations:
   - The photograph on a driver's license or other photo ID submitted by the patient does not resemble the patient.
   - The patient submits a driver's license, insurance card, or other identifying information that appears to be altered or forged.
   - Information on one form of identification the patient submitted is inconsistent with information on another form of identification or with information already in the practice's records.
   - An address or telephone number is discovered to be incorrect, non-existent or fictitious. – The patient fails to provide identifying information or documents.
   - The patient's signature does not match a signature in the practice's records. The Social Security number or other identifying information the patient provided is the same as identifying information in the practice's records provided by another individual, or the Social Security number is invalid.

Respond to Red Flags

If an employee of CDI detects fraudulent activity or if a patient claims to be a victim of identity theft, CDI will respond to and investigate the situation. If the fraudulent activity involves protected health information (PHI) covered under the HIPAA security standards, CDI will also apply its existing HIPAA security policies and procedures to the response.

Procedures:

If potentially fraudulent activity (a red flag) is detected by an employee of CDI:

1. The employee should gather all documentation and report the incident to his or her immediate supervisor (or designated compliance officer/privacy official, if applicable).
2. The supervisor (or designated compliance officer/privacy official, if applicable) will determine whether the activity is fraudulent or authentic based upon the evidence presented.
3. If the activity is determined to be fraudulent, then CDI should take immediate action. Actions may include:
   - Cancel the transaction
   - Notify appropriate enforcement agencies
   - Notify the affected patient
   - Notify affected practitioners
   - Assess impact to practice
4. If a patient claims to be a victim of identity theft:
   - The patient should be encouraged to file a police report for identity theft if he/she has not done so already
   - The patient should be encouraged to complete the ID Theft Affidavit developed by the FTC, along with supporting documentation and send to: https://www.consumer.ftc.gov/articles/pdf-0094-identity-theft-affidavit.pdf
   - CDI will compare the patient's documentation with personal information in the practice's records.

5. If following investigation, it appears that the patient has been a victim of identity theft, CDI will promptly consider what further remedial act/notification may be needed under the circumstances, including:

   - The physician shall review the affected patient's medical record to confirm whether documentation was made in the patient's medical record that resulted in inaccurate information in the record. I f inaccuracies due to identity theft exist, a notation should be made in the record to indicate identity theft.
   - The practice medical records staff will determine whether any other records and/or ancillary service providers are linked to inaccurate information. Any additional files containing information relevant to identity theft will be removed and appropriate action taken. The patient is responsible for contacting ancillary service providers.

6. If following investigation it does not appear that the patient has been a victim of identity theft, CDI will take whatever action it deems appropriate.