Mountain Dental

HIPAA Privacy Rule Policies and Procedures for Colorado

Effective September 23, 2013

These policies are designed to provide covered entities with an outline for how to handle HIPAA-related privacy and security issues. The policies are divided into sections and subsections, with a brief explanation of each at the beginning of each section and subsection.

Page

Patient Requests, Rights and Complaints 1
- Right to request access to PHI 2
- Right to request restrictions on the use or disclosure of PHI 5
- Right to request confidential communications 8
- Right to an accounting of disclosures 9
- Right to request an amendment of PHI 12
- Complaints 15

Internal use/Entity Procedures/External Disclosures 16
- Notice and acknowledgement of Privacy Practices 17
- Permitted uses and disclosures 19
- Patient consent / authorization 21
- Limiting disclosure of PHI 23
- Typical reports and disclosures that do not require authorization 25
- Law enforcement 26
- Judicial proceedings 28
- Disclosures to family and friends 29
- ID and authority verification 30
- Minors 31

Specialized Uses and Disclosures, Special Cases 32
- Research 33
- Limited data sets 35
- De-identification 37
- Marketing 39
- Fundraising 40
- Disclosures after death 41
- Workers' compensation 42
- Sale of PHI 43
- Student immunizations 44
- Psychotherapy notes 45

Business Associates 46
- Business associate agreements 47
- Business associate relationship 49

Breach Notification Policies and Procedures 50
- Identifying a breach of unsecured protected health information 51
- Notification of breach to individual(s) 53

Notification of breach to the media 55
Notification of breach to the Secretary 56

Employment and Training Issues 57
Training of employees 58
Discipline and mitigation for violations 59
Employee health records 61
Whistleblowers and workforce member crime victims 62

Physical and Electronic Handling of PHI 63
Storage and document retention 64
Disposal of documents 66
Email, regular mail, fax, voicemail, and phone messages 67
Computer passwords, access, and other security 68

Patient Requests, Rights and Complaints

HIPAA provides patients with a wide variety of rights regarding the use of and access to their own PHI. This section describes the rights that each patient have, how Mountain Dental will handle patient requests to exercise those rights, and how to handle patient complaints in this area. This section covers the following areas:

1. Right to request access to PHI
2. Right to request restrictions on the use or disclosure of PHI
3. Right to request confidential communications
4. Right to an accounting of disclosures of PHI
5. Right to request an amendment of PHI
6. Complaints

Right to request access to PHI

Policy: Mountain Dental will comply with a patient's request to access the patient's own health records and PHI, as specified in the process outlined below. It is the responsibility of Lead Patient Service Representative or Business Office Manager to receive and process requests for access. If access is denied by Mountain Dental, the patient has the right to review the reason for denial.

Purpose: To ensure that Mountain Dental provides patients with proper access to their PHI.

Form: Request for Access to Records and Response

Process:

Writing requirement:

- Patient requests for access to their own PHI must be in writing.

Denying access to records:

- Mountain Dental may deny patient access, without providing the patient an opportunity to review such decision, in the following circumstances:
    - psychotherapy notes;
    - civil/administrative/or criminal actions;
    - information maintained by a lab, unless access is authorized by CLIA;
    - correctional institutions;
    - research (if the patient has agreed to a temporary restriction to access); or
    - PHI that was obtained by someone other than a health care provider (e.g., a member of the patient's family) with the understanding that it would be kept confidential, and their identification would likely be evident if the PHI is accessed.
- Mountain Dental may also deny access, and a patient may request a review of such decision to deny access, if any of the following apply:
    - Access is likely to endanger the life or physical safety of an individual;
    - The medical records make reference to someone other than a health care provider and access to the records may cause substantial harm to that person; or
    - The request is made by the patient's personal representative and a licensed health care professional has determined that provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

Timeline for granting access:

- Written requests for access to PHI must be acted on within 30 days. If Mountain Dental is unable to comply within the 30 days, a one-time extension of an additional 30 days is allowed if Mountain Dental notifies the patient in writing of the date by which it will comply with the request.
- If the PHI requested is not held by Mountain Dental, but Mountain Dental is aware where the PHI held, the patient must be informed.

Format of PHI provided to patient:

- If patient requests PHI in a non-electronic format, PHI should be in the format requested when possible, or in a readable hard copy (another format is acceptable if agreed to by the patient).
- If patient requests PHI in an electronic format, Mountain Dental must provide the PHI in the electronic format requested by the patient if Mountain Dental maintains PHI electronically in one or more designated record sets.
    - If there are links to data within the designated record set, such data must also be provided to the patient.
    - If the electronic PHI is not readily producible in the electronic format requested by the patient, Mountain Dental must provide the PHI in a readable electronic format agreed to by the patient (e.g., Microsoft Word or Excel, text, HTML or text-based PDF).
- Mountain Dental may choose to provide a summary rather than the complete record if acceptable to the patient.
- Mountain Dental must transmit the PHI (whether paper or electronic) to a person or covered entity designated by the patient pursuant to a patient's request, if the request is in writing, signed by the patient and clearly identifies the designated recipient (an electronic signature is acceptable).
- The patient may review and/or copy the PHI and should be provided a time and place to do so if requested.
- Mountain Dental may charge a reasonable, cost-based fee in accordance with state law to cover only (i) labor costs of copying the PHI; (ii) supplies for creating the paper copy or electronic media, if patient requests the records be provided on portable media; and/or (iii) postage, if applicable. NOTE: There is a $10 duplication fee for patient requests, and this can be processed through Dental Vision.
- If the charge for a summary is extra, patients must be informed in advance and agree to the charge.

Denying access to records:

- The denial must be given to the patient in writing within 30 days of the request for access.
- The denial must include the reason for the denial (and instructions on how the patient may request a review for those denials that include the right to request it).
- The patient must also be given information on how to file a complaint to Mountain Dental and appropriate contact information for the complaint process.
- When patient is denied access to specific PHI, access must be granted to PHI other than that to which the denial is related.
- When a patient requests review of a denial, a licensed health care professional (who was not involved in the denial decision) must conduct the review to determine whether or not the denial will be upheld.
- All patient requests for review must be referred to the designated health care professional in a timely manner.
- The designated health care professional must make their determination within a reasonable amount of time after which the patient must be given written notice of the results of the review.

Right to request restrictions on the use or disclosure of PHI

Policy: Mountain Dental will respond to a patient's request to restrict disclosures of PHI as outlined in the process below. Mountain Dental is not required to comply with all such requests.

Purpose: To be in compliance with the HIPAA Privacy Rule.

Process:

Writing requirement:

- All requests by patients to restrict disclosure of PHI beyond what is required by law or otherwise noted in Mountain Dental's policies must be in writing.
- Examples of such restriction requests would be: requesting that PHI not be disclosed to an outside healthcare provider involved in the patient's treatment or requesting that PHI not be disclosed to a particular employee for billing purposes.

Complying with requests for restriction:

- Mountain Dental is not required to comply with all requests (i.e., those that may result in Mountain Dental's inability to treat the patient or bill for services rendered).
    - One exception: Mountain Dental must comply with an individual's request to restrict the disclosure of PHI to a dental plan for payment or health care operations when the PHI pertains solely to a health care item or service for which the individual has paid Mountain Dental out of pocket in full. Mountain Dental may ask the patient for payment up front before implementing the restriction.
        - Bundled services. In the event the patient requests a restriction with regard to one of several items or services that are bundled for billing purposes, and Mountain Dental cannot unbundle the items or services, Mountain Dental should inform the patient and give the patient the option to restrict and pay out of pocket for the entire bundle. If Mountain Dental unbundles the services, Mountain Dental must counsel the patient on the consequences of doing so (i.e., the dental plan may still be able to identify the services performed based on context).
        - HMOs. If Mountain Dental is prohibited by law (not just contractually) from accepting payment from the patient above the cost-sharing amount, Mountain Dental may inform the patient that he/she must use an out-of-network provider in order to restrict disclosure to the HMO.
- If Mountain Dental agrees to a restriction, it will be bound by the agreement, unless the patient requests or agrees to the removal of the restriction in writing, or Mountain Dental terminates the restriction as provided below.

Process for reviewing requests:

- All requests for restricted disclosure will be processed by the Lead Patient Service Representative or Business Office Manager at the office level to ensure that the ability to treat the patient, bill for services rendered and otherwise perform necessary Mountain Dental functions is not impeded by the requested restriction.
- If the Lead Patient Service Representative or Business Office Manager approves the request, the restrictions must be documented in the health record and appropriate staff must be notified.
- If the Lead Patient Service Representative or Business Office Manager denies the request, the restrictions must be documented in the health record and appropriate staff must be notified. They must also email the details of the request and denial to the Privacy Officer at MDSC.

Denying requests for restriction:

- The Lead Patient Service Representative or Business Office Manager may not give approval to any restrictions of disclosure under the following circumstances:
    - PHI disclosures required by law, including disclosures that are:
        - Related to mandatory reporting
        - Necessary for health oversight activities
        - Required by court order
        - Provided to coroners or medical examiners
        - Public health purposes as defined by state law
    - Other PHI disclosures that do not require patient authorization or that do not require that the patient be given an opportunity to agree or object to the disclosure.

Emergency situations:

- In the case of a medical emergency, when Mountain Dental has previously agreed to restrictions on disclosure of PHI, Mountain Dental may use the PHI as necessary to provide emergency treatment.
- If Mountain Dental discloses PHI to another provider in an emergency, Mountain Dental must request that the provider agrees not to redisclose the PHI to others or use the PHI other than for the emergency.

Termination of restrictions:

- The patient may terminate the restrictions on PHI disclosure in writing or verbally (if verbal, the agreement to terminate should be documented).

- Except as provided below, Mountain Dental may terminate a restriction after Mountain Dental notifies the patient of its intention to do so, but such termination applies only to PHI collected after the restriction is revoked.
    - However, in no event may Mountain Dental terminate a restriction on disclosures to a dental plan for payment or health care operations pertaining solely to an item or service for which patient has paid Mountain Dental out of pocket in full.

Right to request confidential communications

Policy: Mountain Dental will honor all reasonable requests made by a patient for alternative methods of communication.

Purpose: To maintain the confidentiality of communications between Mountain Dental and patients.

Process:

Right to request:

- A patient has a right to request that Mountain Dental use alternative methods for communicating the patient's PHI.
- A Mountain Dental employee may not make an inquiry of the patient as to the reason for the request for alternative methods of communication.

Writing requirement:

- Requests for alternative methods of communication must be made in writing by the patient.

Reviewing requests:

- All requests must be forwarded to the Lead Patient Service Representative or Business Office Manager for review.
- If the request for alternative method(s) of communication affects Mountain Dental's ability to collect payment for services, Mountain Dental should clarify with the patient how payments will be handled.
- If the patient does not clarify how payments will be handled or does not give an alternate address, Mountain Dental may refuse the request.
- If the patient requests that Mountain Dental not use the address on file, Mountain Dental should obtain an alternate address from the patient.
- After review and approval by the Lead Patient Service Representative or Business Office Manager, the request must be noted in the patient's record and appropriate revisions will be made to the patient's contact information as necessary.
- The Lead Patient Service Representative or Business Office Manager will document the name of the individual who made the revision to the patient's information and the date of the revision. They must also email the details of the request to the Privacy Officer at MDSC.

Right to an accounting of disclosures

Policy: Patients have the right to request an accounting of certain disclosures of PHI and Mountain Dental will comply with requests as specified in the process outlined below.

Purpose: To provide information to patients about disclosures of their PHI.

Form(s): Request for Accounting of Disclosures and Response

Process:

Right to request accounting:

- Patients may request an accounting of disclosures to and by Mountain Dental and its business associates of their PHI for a specified period of time up to six years prior to the date of the request.
- Mountain Dental will use the attached "Accounting of Disclosures" checklist to determine which disclosures must be included in the accounting to the patient.

Timeline for providing accounting:

- Mountain Dental must provide the accounting within 60 days of the request.
- A one-time extension of an additional 30 days will be allowed if Mountain Dental notifies the patient in writing as to the reason for the delay and the date by which the accounting will be provided.

Process for providing accounting:

- The Lead Patient Service Representative or Business Office Manager, with assistance from the Privacy Officer at MDSC, will be responsible for receiving and processing all requests for an accounting of PHI disclosures.

Content of accounting:

- The accounting provided for the patient must be in writing and must include the following information for each disclosure:
    - Date
    - Name (and address if known) of the recipient of the disclosure
    - Brief description of the PHI disclosed.
    - Brief statement of the purpose of the disclosure or a copy of the written request for disclosure (if any).

- If multiple disclosures of PHI have been made to the same person or organization for the same purpose (other than for the excepted disclosures), then only the accounting for the first disclosure must include the information noted above.
- In the case of multiple disclosure accounting, the frequency and number of disclosures, date range of the accounting period and date of the last disclosure must also be included.
- A "short cut" accounting is allowed when a patient's information may have been disclosed for research involving more than 50 people when the authorization requirement has been waived. The following information must be provided:
    - Name of protocol
    - Description of research and information disclosed
    - Date of disclosure
    - Information about the research sponsor
    - Statement that PHI may have been disclosed
- If the "short cut" accounting method is used and it is reasonably likely that PHI will be disclosed, Mountain Dental must assist in contacting the sponsor of the research when requested.

Fees:

- No charge may be made for the first accounting request fulfilled in any 12-month period.
- A charge of $10 will be charged for each additional accounting during the same 12-month period. Employees can use the duplication charge that is in Dental Vision.
- If Mountain Dental decides to charge the patient for the additional accountings, Mountain Dental must notify the patient of the charge in advance and give the patient an opportunity to retract or limit the request in order to reduce the charge.

Restrictions on accounting:

- Law enforcement or health oversight agencies can request a suspension of the accounting of disclosures to that agency. Such requests can be written or verbal. If the request is written, it must specify the time period and reason for the suspension. If the request is verbal, suspension is limited to 30 days unless the agency submits a written statement that states an accounting will be reasonably likely to impede the agency's activities and specifies how long the suspension will be in force it. Employees contacted by law enforcement must notify the Privacy Officer immediately.

Accounting of Disclosures Checklist

Mountain Dental MUST account for the following types of disclosures:

- ☐ For public health activities (e.g., for disease control, vital statistics reporting, etc.)
- ☐ For FDA-regulated products or activities
- ☐ For purposes of reporting abuse (child abuse, neglect, others as required by state law)
- ☐ For health oversight activities (e.g., to an agency for investigations, licensure and disciplinary actions, etc.)
- ☐ For judicial and administrative proceedings (e.g., in response to a court order)
- ☐ For law enforcement purposes (e.g., reporting gunshot wounds, for identification purposes)
- ☐ Regarding victims of a crime
- ☐ Regarding the reporting crime on the premises
- ☐ Regarding the reporting of crime in emergencies
- ☐ For the provision of information to coroners and medical examiners
- ☐ For organ, eye, or tissue donation purposes
- ☐ For research purposes (special accounting rules apply in research context)
- ☐ In order to avert a serious threat to health or safety
- ☐ For military/veterans activities (e.g., for armed forces personnel to assure proper execution of a military mission)
- ☐ For protective services of the President, foreign heads of state, etc.
- ☐ For workers compensation purposes
- ☐ Disclosures to or by business associates for any of the above purposes

Mountain Dental does NOT need to account for disclosures made under the following circumstances:

- ☐ Information has been de-identified
- ☐ For treatment, payment, or health care operations purposes
- ☐ Pursuant to an authorization
- ☐ To the patient or someone involved in the patient's care
- ☐ For a facility directory
- ☐ For national security or intelligence purposes (e.g., to authorized federal officials for lawful intelligence or counter-intelligence)
- ☐ To law enforcement officials/correctional institutions with custody of the patient
- ☐ Disclosure occurred more than six years from the date of the request for accounting
- ☐ Meets the criteria for a limited data set
- ☐ If patient has agreed to suspend the right to an accounting
- ☐ Incidental disclosures (e.g., statements in a waiting room that may have been overheard)

NOTE: THIS IS NOT A LIST OF PERMISSIBLE DISCLOSURES! THIS LIST DESCRIBES THE INSTANCES WHERE HIPAA REQUIRES THAT A PROVIDER ACCOUNT FOR A PARTICULAR DISCLOSURE. WHETHER A DISCLOSURE IS PERMISSIBLE DEPENDS ON STATE LAW AND HIPAA.

Right to request an amendment of PHI

Policy: Patients have the right to request amendment of their health records, and Mountain Dental will follow the process outlined below when considering the amendment request.

Purpose: To be in compliance with the Privacy Rule of HIPAA.

Form(s): Request for Amendment of Records and Response

Process:

Writing requirement:

- Patient requests for amendment of a health record must be made in writing.
- The patient must provide the reason for requesting the amendment.

Timeframe:

- Mountain Dental must respond to the request within 60 days from receipt of the request.
- A one-time extension of an additional 30 days will be allowed if Mountain Dental notifies the patient in writing of the reason for the delay and the date by which action will be taken on the request.

Process for approving/denying amendment:

- The Privacy Officer is responsible for receiving and processing requests for amendments to health records.
- Mountain Dental has the right to refuse the amendment request under the following circumstances:
    - Mountain Dental determines the information in the health record is accurate and complete;
    - The health record was not created by Mountain Dental, unless the patient provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the request for amendment;
    - The PHI the patient wishes to amend is not part of the health record; or
    - The PHI is the type of information to which the patient does not have a right of access (e.g., psychotherapy notes).
- If Mountain Dental grants the request for amendment in whole or part:
    - The patient should be informed that the amendment is accepted.
    - The Privacy Officer, along with a health care professional, should make the amendment to the health record. (The amendment may be added to the record

itself, or the record may be flagged with information on where to locate the amended information).

- Mountain Dental must obtain from the patient a list of the persons who have received the health record and need the amendment.
- Mountain Dental must obtain the consent of the patient to notify the persons the patient has identified for the purpose of informing them of the amendment.
- Mountain Dental must make reasonable efforts to inform and provide the amendment within a reasonable time to the (i) persons identified by the individual and (ii) persons, including business associates, that Mountain Dental knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely upon the information, to the detriment of the patient.

- Denials of amendment must be given to the patient within 60 days (unless Mountain Dental has exercised its right to a one-time extension of 30-days as described above) and must include the following information:
  - The reason for the denial.
  - The patient's right to submit a written statement disagreeing with the denial and where to file the statement.
  - The patient's right to request that Mountain Dental provide the request for amendment and denial with any future disclosures of PHI that is the subject of the denied amendment; and
  - Information regarding how the patient may complain to the Privacy Officer, including the name and telephone number of the Privacy Officer.

Disputed amendments

- If the amendment is denied, the patient may submit a written statement of reasonable length disagreeing with the denial and stating the basis for disagreement.
- Upon receipt of the statement of disagreement, the Privacy Officer may, in his or her discretion, prepare a rebuttal. Mountain Dental must give the patient a copy of the

Disclosure of PHI after request is denied:

- The amendment request, the denial (if any), the statement of disagreement (if any) and the rebuttal (if any), must all be added to the applicable PHI and kept in the patient's medical record.
- If Mountain Dental discloses PHI after a request for amendment of that PHI has been denied and a statement of disagreement submitted, both documents (and a rebuttal document, if any), or a summary document of the information, must be included with the PHI.

- If an amendment request is denied, but the patient does not submit a statement of disagreement, the patient has the right to request that both the amendment request and the denial are included with any future disclosures of the affected PHI. Mountain Dental will comply with such requests, but if the future disclosure is made under a HIPAA standard transaction which does not permit inclusion of the additional information, Mountain Dental may choose to transmit the material separately. (Statements of disagreement and rebuttal, if any, may also be transmitted separately as necessary).

Amendment requests from other health care providers:

- If Mountain Dental receives notification from another provider or covered Mountain Dental of an amendment to PHI which Mountain Dental has in its possession, the PHI must be amended as applicable and the patient must be notified of the amendment.
- Mountain Dental will retain the documentation of all requests for amendment to records.

Complaints

Policy: All complaints received regarding HIPAA will be addressed in a timely manner, following the process outlined below.

Purpose: To demonstrate Mountain Dental's commitment to maintaining the confidentiality of PHI.

Process:

- All complaints related to HIPAA should be directed to the Privacy Officer within 24 hours of receipt.
- Complaints that are given verbally should be summarized in written form by the individual taking the complaint and forwarded to the Privacy Officer within 24 hours of receipt.
- Complaints will be handled by the Privacy Officer, in consultation with the administrator and Mountain Dental's legal counsel.
- All complaints and their disposition will be documented by the Privacy Officer.
- Mountain Dental and its employees will not intimidate, threaten, coerce, discriminate against or otherwise retaliate against any patient filing a complaint.
- Mountain Dental will not take any action against any employee or other individual who files a complaint, participates in an investigation or oppose policies by Mountain Dental that they believe in good faith to be in violation of the Privacy Rule, as long as the person is acting in a reasonable manner and their actions do not of themselves include an unlawful disclosure of PHI.

Internal and External Uses and Disclosures of PHI

One of the main goals of the HIPAA regulations was to create a minimum standard for the internal use and external disclosure of PHI by health care organizations. The Privacy Regulations have some very specific requirements, and Mountain Dental must follow more stringent state laws as well. This section covers the following areas, which address internal uses, external disclosures, and Mountain Dental procedures and HIPAA provisions that affect both:

1. Notice and acknowledgement
2. Permitted uses and disclosures
3. Patient consent/authorization
4. Typical reports and disclosures that do not require authorization
5. Law enforcement
6. Judicial proceedings
7. Limiting disclosure of PHI
8. Disclosures to family and friends
9. ID and authority verification
10. Personal representatives
11. Minors

Notice and acknowledgement of privacy practices

Policy: A written notice of the uses and disclosures of PHI that may be made by Mountain Dental (a "Notice of Privacy Practices" or "Notice") will be provided to every patient with whom Mountain Dental has a direct treatment relationship. The Notice will also describe the patient's rights and Mountain Dental's legal duties with respect to PHI.

Purpose: To provide patients with notice regarding Mountain Dental's use and disclosure of PHI, their rights and Mountain Dental's legal duties with respect to PHI.

Form(s): Notice of Privacy Practices and Acknowledgement of Notice of Privacy Practices and Authorization for PHI Disclosure

Process:

Distributing notices of privacy practices

- A written Notice of Privacy Practices will be in place at Mountain Dental's location(s).
- Mountain Dental will make a good faith effort to provide a copy of the notice of privacy practices (the "notice") to every patient with whom it has a direct treatment relationship before or at the time of their first service delivery by Mountain Dental. Mountain Dental need only provide the notice to each patient one time; subsequently, the notice must be available to every patient upon request.
    - If the patient presents in person for the first service delivery, a written copy of the notice will be given to the patient at that time.
    - If the first service delivery to the patient is made by telephone or electronic mail, a copy of the privacy notice must be mailed (via regular or email, as applicable) on the day of the service delivery.
    - Telephone contact with patients solely for the purpose of scheduling an appointment is not considered a "service delivery."
- Mountain Dental will provide a copy of the notice to any individual upon request.
- Persons who receive a copy of the privacy notice via electronic mail are also entitled to receive a paper copy upon request.
- Mountain Dental will post the privacy notice in a prominent location at all Mountain Dental's sites (and electronically on Mountain Dental's website, if available).

Patient acknowledgement of notice of privacy practices

- Mountain Dental will make a good faith effort to obtain written acknowledgment from the patient that the patient received a copy of the notice. Mountain Dental will keep the acknowledgement with the patient's health record.

- If the patient refuses or is unable to acknowledge receipt of the copy of the notice (or does not return a mailed acknowledgment form for the notice), Mountain Dental shall document the good faith effort to obtain acknowledgment and the reason that it was not obtained.
- The acknowledgement and/or documentation of the good faith effort must be retained according to the policy on Retention of Documents.
- Mountain Dental may continue to treat the patient even though the patient has refused or is unable to acknowledge receipt of the N otice.
- In an emergency treatment situation, distribution of the notice may be delayed until a reasonable time after the emergency ends. Mountain Dental need not obtain an acknowledgement of the receipt of the notice in emergency situations, even after the emergency ends.

Changes to the notice of privacy practices:

- Mountain Dental reserves the right to change its notice of privacy practices. The Privacy Officer will update the notice and is responsible for posting the revised notice and educating staff, as appropriate.
- Updated notices of privacy practices do not have to be distributed to patients who have previously received a notice, except upon request.
- Mountain Dental must provide a copy of the Notice to any individual who does not have a direct treatment relationship with Mountain Dental, if requested, but Mountain Dental is not required to obtain acknowledgement of receipt of the notice from those individuals.

Permitted uses and disclosures

Policy: Mountain Dental will use and disclose PHI as necessary for purposes of treatment, payment and health care operations both within Mountain Dental and outside of Mountain Dental. When required, Mountain Dental will use and disclose only the minimum necessary information to accomplish the purpose of the use or disclosure, as permitted by HIPAA and applicable state law.

Purpose: To ensure that PHI is used and disclosed appropriately for purposes of operating Mountain Dental.

Process:

- Treatment, payment, and health care operations. Mountain Dental may use and disclose PHI as necessary for its own treatment purposes, payment purposes, and its health care operations.
    - Treatment includes the provision, coordination, and management of care, consultations relating to a patient, or referrals to another health care provider.
    - Payment includes Mountain Dental activities (including billing and collection) to obtain or provide reimbursement for the provision of health care.
    - Health care operations include many of the activities necessary to operate Mountain Dental, including health record storage, quality assurance and improvement, reviewing practitioner competence or qualifications, conducting training programs, conducting or arranging for medical review, legal services, audits, business planning and development, and business management and general administrative activities.
    - Mountain Dental may use PHI for these activities, but, except for treatment purposes, should use and disclose only the minimum amount of information necessary to accomplish the purpose of the disclosure. For example, in disclosing PHI for payment purposes, Mountain Dental should disclose only the PHI necessary to payment of a particular claim.
- "Incidental disclosures" are not considered violations of the Privacy Rule These are disclosures that occur as an incident to a use or disclosure that is otherwise permitted or required by the Privacy Rule, so long as Mountain Dental also complies with the minimum necessary requirements and the requirement of implementing appropriate safeguard:
    - *Technical safeguards.* Example: Passwords, firewalls, encryption, etc.
    - *Administrative safeguards*. Example: Nurses placing charts in racks so that PHI is turned away from passersby; receptionists speak in a soft voice, etc.
    - *Physical safeguards*. Example: Locking doors where records or other PHI is stored, privacy screens on computers, etc.

- Although incidental disclosures are not required to be included in a requested accounting of disclosures, those disclosures that are the result of an error or neglect (e.g., faxing PHI to the wrong fax number) are not considered "incidental disclosures" and must be included in a requested accounting and may require notifying the patient (see Breach notification policy).
- Disclosure of PHI for the treatment, payment or healthcare operations purposes of another covered Mountain Dental
    - PHI may be disclosed for the treatment activities of another health care provider, the payment activities of another health care provider or covered Mountain Dental, and for certain health care operations of another covered Mountain Dental in the following circumstances:
        - Both Mountain Dental and the other covered Mountain Dental have or have had a relationship with the individual who is the subject of the PHI disclosure.
        - If the relationship between the individual and the other covered Mountain Dental has ended, only the PHI which was related to the past relationship may be disclosed.
        - Health care operations that are included for this purpose include quality assessment and improvement activities, population-based activities relating to reducing health care costs, case management, training programs, licensure and certification, accreditation, credentialing, fraud and abuse detection and compliance.
        - Other health care operations, such as financial auditing, are not included for this purpose.
- The "minimum necessary requirement still applies for disclosures for payment and health care operations.
- If an employee has questions as to whether or not the requested disclosure qualifies under this policy, the Privacy Officer at MDSC should be consulted prior to the disclosure being made.

Patient consent/authorization

Policy: Disclosures of PHI for treatment, payment and/or health care operations that are not otherwise permitted by the Privacy Rule will be made only as specified in the process outlined below and as permitted by state law.

Purpose: To be in compliance with the Privacy Rule.

Form: Acknowledgement of Notice of Privacy Practices and Authorization for PHI Disclosure

Process:

- HIPAA requires patient authorization for disclosures of PHI for purposes other than those specifically permitted by the Privacy Rule.
- When a patient requests disclosure of PHI in person, the authorization form should be completed and signed. The patient does not need to fill out an authorization to receive a copy of his or her own PHI.
- When a patient requests disclosure of PHI by telephone, they should be offered the option to have an authorization form mailed or faxed to them to complete and return, or the patient may come in personally to complete the form.
- If the patient presents with his or her own authorization form, it must meet the criteria for authorizations outlined in this policy.
- Third parties requesting disclosure of PHI should be informed that an authorization from the patient must be obtained.
- A valid authorization must be written in plain language and must include the following:
    - Specific description of the PHI to be used;
    - Name or specific identification of the patient or other person(s) authorized to make the requested disclosure;
    - Name or specific identification of the recipient(s) of the PHI;
    - The purpose of the requested use/disclosure ("at the request of the individual" will be sufficient if that is the case);
    - Expiration date of the authorization or of the event related to the purpose (e.g., "end of research study");
    - Signature of the patient (or if signed by the patient's personal representative, a description of their authority to act for the patient) and date signed;
    - Statement regarding the requestor's right to revoke the request and instructions on how to request revocation;
    - Statement regarding whether or not treatment may be conditioned on the patient's signing the authorization (and the potential consequences for those situations when it can be — e.g., treatment provided in order to create PHI

specifically for disclosure to a third party (such as a fitness for work evaluation) may be conditioned on the patient's provision of an authorization authorizing disclosure to that third party;

- Statement regarding the potential for the information to be re-disclosed when no longer under the control of Mountain Dental;
- For authorizations to use or disclose PHI for marketing purposes, if applicable: Statement that Mountain Dental received financial remuneration in exchange for making the marketing communication.
- For authorizations to sell PHI, if applicable: Statement that Mountain Dental received direct or indirect remuneration in exchange for the sale.

- A copy of the signed authorization must be given to the requestor.
- If the employee has concerns over the authorization form used or the PHI requested for disclosure, they should check with the Privacy Officer for approval prior to disclosing the information.
- Treatment may not be conditioned on the obtaining of an authorization for disclosure of PHI with the exceptions of research-related treatments or health care provided solely for the purpose of creating PHI for disclosure to a third-party.
- Patients have the right to revoke an authorization in writing at any time, and the revocation prevents further disclosures of PHI, except when Mountain Dental has already acted in reliance on the authorization.
- Authorizations must be documented and retained according to Mountain Dental's policy on retention of documents.
- An authorization may not be combined with documents, with the following exceptions:
  - Except for authorizations to use or disclose psychotherapy notes, any two or more unconditioned authorizations may be combined (e.g., authorization for the use/disclosure of PHI for marketing purposes and the sale of PHI);
  - An authorization for psychotherapy notes may be combined only with another authorization for psychotherapy notes; and
  - A conditioned and unconditioned authorization for research purposes may be combined, so long as the conditioned and unconditioned portions are clearly differentiated.

Limiting disclosure of PHI

Policy: Mountain Dental shall make reasonable efforts to limit the access to and uses of PHI by employees, as well as disclosures outside Mountain Dental to a limited data set or the minimum necessary for the purpose of the access, use, or disclosure.

Purpose: To maintain the confidentiality of a patient's health information.

Definitions:

"Minimum necessary" means that the minimum amount of PHI that is necessary to achieve the specified goal based on Mountain Dental's size, health records practices and other reasonable considerations.

Process:

- Any employee, provider or contracted worker who needs access to PHI to perform his or her assigned job duties have been identified by Mountain Dental.
- Providers, clinical staff, contract workers and all employees involved in the provision or supervision of patient care will have access to the complete medical record for treatment purposes.
- For all other purposes, Mountain Dental and the individuals who need access to PHI for their job duties will limit any use or disclosure of PHI to the minimum necessary required to perform the assigned duties.
- When fulfilling a request for disclosure of PHI (other than for the purposes outlined below), employees should make a reasonable effort to disclose only the minimum amount of information necessary required to accomplish the purpose of the disclosure. All other Mountain Dental policies and procedures related to disclosures of PHI must also be followed.
- Routine and/or recurring requests for disclosure of PHI (e.g., for payment purposes) shall be handled in such a way as to disclose the minimum amount of information necessary to accomplish the purpose of the disclosure. Requests from other covered entities, business associates and researchers/Institutional Review Boards/Privacy boards may be relied upon as being for the minimum necessary for the purpose of their requests.
- Non-routine disclosures must be reviewed to determine the minimum amount of information necessary to accomplish the purpose of the disclosure.
- The minimum necessary standard does not apply to the following types of disclosures:
    - Disclosures made for requests by a health care provider for treatment purpose, disclosure of mental health information by a mental health professional must be limited to the information needed to provide professional services;
    - Uses and disclosures by or to a patient of his or her own PHI;

- Disclosures made under a valid authorization;
- Disclosures to public officials when disclosure is permitted under law and the official represents that the information requested is the minimum required for the purpose;
- Disclosures made to other covered entities as defined and allowed by HIPAA;
- Disclosures made to Mountain Dental's employees or its business associates, when the requesting party represents that the information requested is the minimum necessary for the purpose of the request;
- Disclosures made to researchers who are compliant with HIPAA and with Mountain Dental*'s* policies;
- Disclosures made to the Secretary of Health and Human Services ("HHS") for compliance and enforcement of the Privacy Rule; and
- Disclosures required for compliance with the other HIPAA provisions, including the Transactions Rule and the Security Rule.

- If an employee is requested to disclose PHI to another covered entity for payment or certain health care operations purposes, only the minimum necessary PHI required for the stated purpose should be disclosed, unless the disclosure meets one of the exceptions described above. The employee may rely on the request from the covered entity as meeting the minimum necessary standard and does not need to perform further analysis.
- When Mountain Dental requests PHI from another covered entity, Mountain Dental should request only the minimum necessary information, except where such requirements do not apply, as described above.

Typical reports and disclosures that do not require authorization

Policy: Employees will disclose PHI as required by state and federal law for certain public purposes.

Purpose: To comply with the Privacy Rule regarding disclosure of PHI for certain public purposes.

Process:

- In addition to disclosures for treatment, payment and health care operations, PHI may be disclosed without an authorization from the patient for the following purposes:
    - Public health activities — disclosure may be made to authorized agencies for disease reporting, vital statistics and other public health reasons as required by state law.
    - FDA-regulated products — disclosure may be made to authorized individuals/agencies.
    - Child or adult abuse or neglect — Mountain Dental will report all suspected child or adult abuse or neglect to authorities as required by state law.
    - Health oversight — disclosures may be made to agencies for health care oversight activities related to the health care system, government benefit programs, fraud and abuse and civil rights (e.g., audits, investigations, licensure, disciplinary action), with the exception of certain situations where the individual is the subject of the investigation or other activity. Employees should immediately refer all requests from government agencies for PHI related to health oversight activities to the Privacy Officer (and/or legal counsel) for review prior to disclosure.
    - HIPAA allows disclosures for various public safety, disaster relief and other specialized government functions (e.g., military and veterans' activities, national security and intelligence, protective services for the President of the United States and other heads of state, correctional institutions and law enforcement custody activities), when permitted by state law.
    - Coroners and funeral directors — HIPAA allows disclosures of PHI to coroners, medical examiners, and funeral directors in accordance with state law.
    - Cadaveric organ, eye or tissue donation — HIPAA allows disclosures of PHI to entities engaged in procurement, banking, or transplantation of organs in accordance with state law.
- Mountain Dental employees should consult with the Privacy Officer if there is any doubt or question about HIPAA or state law compliance with regard to any of these disclosures. In some cases, state law may require that disclosure of PHI for these purposes is subject to additional protective measures.

Law enforcement

Policy: Mountain Dental will make disclosures of PHI for a law enforcement purpose only as required/permitted by law.

Purpose: To be in compliance with the Privacy Rule and applicable state laws.

Process:

- PHI may be disclosed for law enforcement purposes as required by a court order, warrant, subpoena, summons, or other administrative request, if permitted by state law. In the case of an administrative request, the PHI disclosed must be relevant to the law enforcement inquiry, specific and limited in scope to the purposes of the request, and may be disclosed only if de-identified information could not reasonably be used instead.
- PHI may be disclosed for law enforcement purposes to report certain injuries if required by state law (e.g., reporting gunshot wounds).
- PHI may be disclosed for law enforcement purposes, in response to a law enforcement official's request for the information, to provide information regarding a patient's identification or location (e.g., if the patient is a fugitive), if permitted by state law. (The information that can be disclosed is limited to the following: name, address, date or place of birth, Social Security number, blood type/Rh factor, type of injury, date/time of treatment or death, and/or distinguishing physical characteristics.)
- PHI may be disclosed to provide information regarding crime victims for law enforcement purposes if permitted by state law and if the victim agrees to the disclosure. If the victim is not able to agree because of incapacity or other emergency, disclosure may be made if the following conditions are met:
    - the information is needed to determine if someone has violated the law,
    - the information is not intended to be used against the patient,
    - the law enforcement official states that it is needed immediately and delay may adversely affect the law enforcement activity,
    - the disclosure is deemed by professional judgment to be in the patient's best interests.
- PHI may be disclosed for reporting a crime on the premises of Mountain Dental if permitted by state law and if Mountain Dental in good faith believes the PHI constitutes evidence of criminal conduct that took place on the premises.
- PHI may be disclosed if required by state law for known or suspected abuse of children.
- PHI may be disclosed for other types of abuse, neglect or domestic violence to a government authority, including a social service or protective services agency, who is authorized by law to receive the reports, if:
    - the disclosure is required by law;
    - the patient agrees; or

- if the disclosure is permitted (but not required) by state law, and the disclosure is believed, in the professional judgment of Mountain Dental staff, to be necessary to prevent serious physical harm to the patient or others, or if the patient is incapacitated and unable to agree, PHI may be disclosed if law enforcement officials state that the PHI is not intended for use against the patient and a delay may adversely affect the law enforcement activity.

- If PHI is disclosed under these provisions, the patient must be informed of the disclosure, unless doing so, in the professional judgment of Mountain Dental staff, would put the patient at risk of serious physical harm, or if the disclosure would be made to a personal representative believed responsible for the abuse.

Judicial proceedings

Policy: Mountain Dental will make disclosures of PHI for judicial proceedings or law enforcement purpose only as required/permitted by law.

Purpose: To be in compliance with the Privacy Rule and applicable laws.

Process:

- PHI may be disclosed for judicial/administrative proceedings as required by a court order or administrative tribunal order. The PHI disclosed should be only that which is required by the order.
- PHI may be disclosed for judicial/administrative proceedings in response to a subpoena, discovery request, or other lawful process if the requestor provides "satisfactory assurance" that the patient has been notified of the request, or that the requestor has made a reasonable effort to obtain a protective order.
- Employees must consult with the Privacy Officer immediately upon receipt of a subpoena, and may not disclose any information without direction from the Privacy Officer.

Disclosures to family and friends

Policy: PHI may be disclosed to individuals involved in the direct care of the patient, without specific patient authorization.

Purpose: To allow for appropriate access to the medical record for treatment purposes.

Process:

- PHI that is directly relevant to patient care may be disclosed to family, close personal friends or other individuals identified by the patient that are directly involved in the patient's care.
- If the patient is present, PHI may be disclosed if the patient agrees or does not object when given the chance to do so.
- If the patient is not present, or is incapacitated or otherwise unable to agree or object, staff may disclose PHI if deemed by professional judgment that it is in the patient's best interest to do so.
- PHI may be also disclosed to inform those involved in patient care of the patient's location, general condition or death, as long as the other criteria in this policy is met.

ID and authority verification

Policy: Mountain Dental will take reasonable steps to verify the ID and authority of individuals requesting PHI.

Purpose: To prevent unauthorized disclosures of PHI.

Process:

- If a patient has consented to or authorized the disclosure of his or her PHI, Mountain Dental encourages the PHI be mailed to the address specified by the patient. If the patient insists the PHI be physically picked up, employees must check the verification of the ID of the person to whom the disclosure is made to ensure that the disclosure of the PHI is appropriate.
- If the PHI is requested by the patient, employees must check the verification of the patient's ID to ensure that the disclosure of the PHI is appropriate.
- In the case of a subpoena or similar administrative request or court order, the matter should be immediately referred to the Privacy Officer, who may refer the question to the Compliance Officer and/or legal counsel.
- If the individual requesting the disclosure has an authorization signed by the patient, Mountain Dental may assume that the authorization is valid unless there is a reason to suspect that it is not.
- If a public official requests PHI for a purpose not requiring authorization (e.g., for a disease registry), the ID of the official should be verified. If the individual requesting PHI makes the request in person, the employee should ask to examine the requestor's identification or credentials. If the request is made in writing, Mountain Dental should require that it be submitted on the official letterhead of the public office held.
- The authority of a public official requesting the disclosure of PHI must also be verified. Mountain Dental will request a statement (written if possible) of the legal authority under which the information is requested.
- If an individual states that he or she has legal authority to act on a patient's behalf (such as a guardian or conservator), Mountain Dental should require documentation of that authority and refer the individual to the Privacy Officer, who may refer the question to the Compliance Officer and/or legal counsel.
- If an individual who is a federal or state government agent arrives to conduct an investigation, the employee should immediately contact the Compliance Officer at the Support Center.
- If an employee has reason to suspect the ID or authority of anyone making a request for disclosure of PHI, the matter should be discussed with the Compliance Officer and the employee should not make the disclosure without Compliance Officer approval.

Minors

Policy: Mountain Dental will use and disclose the PHI of minors only as specified in the process outlined below. For purposes of this policy, "minors" refers to individuals under the age of 18, or as otherwise defined by state law.

Purpose: To maintain the confidentiality of the PHI of minors and be in compliance with the Privacy Rule and all other existing laws.

Process:

- Mountain Dental will follow state law related to the uses and disclosures of the PHI of minors.
- Parents/legal guardians as personal representatives:
    - Parents/legal guardians generally are permitted by state law to act on behalf of their minor children in making health care decisions (i.e., acting as the "personal representative"). When parents/legal guardians are acting as personal representatives, they may make decisions for their minor children related to the uses and disclosures of the minor's PHI.
    - A minor may make his/her own health care decisions, and the parents/legal guardians should not be considered the minor's personal representative, under the following circumstances:
        - the minor has the right to consent and no other consent is required under state law
        - the minor has the right to obtain a specific health care service and consent is provided by the minor, a court, or another as authorized by state law
        - the parent/legal guardian has agreed to confidentiality between the minor and the health care provider for a specific health care if permitted by state law.
- Disclosure of the PHI of minors:
    - Mountain Dental may disclose PHI of minors to a parent/legal guardian or others acting in their place when state law (or applicable case law) requires or permits such disclosures.
    - Mountain Dental may not disclose PHI of minors to a parent/legal guardian or others acting in their place when state law (or applicable case law) prohibits such disclosures.
    - Mountain Dental will follow all other privacy policies and procedures related to uses and disclosures of PHI unless in conflict with state law related to the PHI of minors.
- When an employee is not certain whether PHI should be disclosed or provided to a parent or legal guardian, the employee should contact the Privacy Officer.

Specialized Uses and Disclosures, Special Cases

There are some issues that HIPAA deals with that will not affect all covered entities. This section addresses the following more specialized areas:

1. Research
2. Limited data sets
3. De-identification
4. Marketing
5. Fundraising
6. Disclosures after death
7. Workers compensation
8. Sale of PHI
9. Student immunizations
10. Psychotherapy notes

Research

Policy: PHI may be disclosed for research purposes only as specified in the process outlined below and when permitted by state law. Internal research activities (e.g., quality improvement) that are not planned to be published are not subject to the requirements of this policy.

Purpose: To be in compliance with the Privacy Rule.

Process:

- PHI may only be disclosed for research when one of the following four criteria is met:
    1. The patient has provided a HIPAA-compliant written authorization.
        - A written authorization of disclosure of PHI for research may be combined with another written permission for the same or another research study (e.g., consent to participate in the research study).
        - Research-related treatment may be conditioned on the patient's signing an authorization to release the treatment information for research purposes.
        - If Mountain Dental conditions the provision of research related treatment on the provision of one of the authorizations in a compound authorization, the compound authorization must clearly differentiate between the conditioned and unconditioned components and provide the patient with an opportunity to opt in to the research activities described in the unconditioned authorization.
    2. An Institutional Review Board ("IRB") or Privacy Board has authorized and provided documentation supporting an alteration to or waiver of the authorization requirement.
    3. The researcher is seeking disclosure of the PHI only for purposes preparatory to research/research protocol, the PHI will not be removed from Mountain Dental, and the PHI is necessary for the research purposes.
    4. The researcher is seeking disclosure of the PHI only for purposes of research related to decedents, provides documentation of the request and of the decedent's death, and the PHI is necessary for the research purposes.
- Documentation required for IRB/Privacy Board alteration to or waiver of authorization:
    - Identity of the board
        - The privacy board must have members of varying backgrounds and with the ability to determine how invasive to privacy the research will be
        - There must be at least one board member who is not affiliated with or related to a person affiliated with Mountain Dental or the research Mountain Dental

        - The board must not have any members that would have a conflict of interest involving the project.
    - Date when the alteration or waiver of authorization approved.
    - Description of the PHI needed.
    - Statement regarding the receipt of the approval and that applicable procedures were followed
    - Authorized board signature.
    - Statement that the following waiver criteria have been met for use and disclosure of the PHI:
        - There is no more than minimal risk to the privacy of the individual, based on, at least, the following elements:
            - An adequate plan to protect identifiers from improper use and disclosure
            - An adequate plan to destroy the identifiers at the earliest opportunity consistent with the research, unless there is a health or research justification or a requirement under law not to do so
            - Adequate written assurances that the PHI will not be reused or disclosed except as required by law, for authorized oversight of the research study, or for other permitted research.
- Statement that the research could not practicably be conducted without the waiver or alteration and without access to and use of the PHI.

Limited data sets

Policy: PHI may be disclosed for purposes of research, public health or health care operations when it has been converted to a limited data set as defined in the process outlined below and Mountain Dental has executed a data use agreement with the recipient.

Purpose: To allow for certain research, public health and health care operations activities while maintaining the confidentiality of PHI.

Process:

- PHI may be disclosed for research, public health and health care operations purposes as part of a limited data set without a patient's authorization, if the following components have been removed from the PHI:
    - Name
    - Street address (but not town/city, state, zip code)
    - Telephone/fax number(s)
    - Email address
    - Social Security number
    - Certificate/license number(s)
    - Vehicle identification/serial number(s)
    - URLs and IP address(es)
    - Full-face photo(s) and other comparable image(s)
    - Medical record number
    - Health plan beneficiary/member number and other account number(s)
    - Device identification/serial number(s)
    - Biometric identifier(s) (e.g., fingerprint/voice print).
- The following information does not need to be removed:
    - Admission, discharge and service date(s)
    - Date of death
    - Age (including months, days or hours), including birth date if Mountain Dental and the researcher agree that it is needed for purposes of the research
    - Town/city, state, 5-digit zip code.
- At the time of the disclosure, a data use agreement must be obtained from the recipient of the limited data set.

- The data use agreement may be in the form of a contract, a memo of understanding or, for internal use, an agreement signed by the employee. All data use agreements must meet the following criteria:
    - It must establish permitted uses and disclosures of the limited data set that are consistent with the purpose of the research, public health, or health care operations activity
    - It must contain language assuring that the recipient will use appropriate safeguards to prevent uses or disclosures of the information other than as permitted by the Privacy Rule or otherwise required by law
    - It must limit who can use or receive the limited data set
    - It must require the recipient to agree not to re-identify or contact the individual subject
    - It must include a requirement to report any improper use or disclosure of which the recipient becomes aware.
- If Mountain Dental is the recipient of PHI under a data use agreement, all provisions of the agreement must be adhered to.
- If an employee knows of a suspected violation of any data use agreement, it must be reported to the Privacy Officer.
- If the Privacy Officer is not successful in fixing the problem, the disclosure of PHI will be discontinued and the problem will be reported to the Secretary of Health and Human Services.
- Limited data sets are also subject to the minimum necessary requirements. Employees may rely on the requested disclosure as meeting the minimum necessary requirements unless they have reason to suspect that it does not.
- Employees must verify the validity of all limited data sets with the privacy officer *(or designee)* prior to disclosures.

De-identification

Policy: PHI that has been "de-identified" is no longer classified as PHI. Mountain Dental may disclose information that meets the criteria of "de-identified" information for any purpose without any consent or authorization from the patient.

Purpose: To allow for disclosures of information for necessary purposes when all identifying information has been removed.

Process:

- To be considered de-identified (and no longer PHI), the information must meet one of the following criteria:
    - A qualified statistical expert determines familiar with rendering information not individually identifiable determines that the risk is very small that the information could be used by an anticipated recipient of the information to identify an individual who is the subject of the information; or
    - The information does not contain any of the following identifiers:
        - Name
        - Geographic subdivisions smaller than a state, including zip code*
        - Date elements (except year)
        - Telephone/fax number(s)
        - Email address
        - Social Security number
        - Medical record number
        - Health plan beneficiary number and other account number(s)
        - Certificate or license number(s)
        - Vehicle identification and serial number(s)
        - Device identifier and serial number(s)
        - URLs and IP addresses
        - Biometric identifiers (e.g., finger and voice prints)
        - Full face photographic images
        - Any other unique identifying characteristic(s) or code(s) (other than those established by an organization to permit re-identification).

      *(*except first 3 digits of zip code, as long as the unit formed by combining all zip codes with the same first 3 digits contains more than 20,000 people)*

- A “dummy” identifier may be used when disclosing data to an external requestor so that the Mountain Dental may re-identify the information at a later date, if the following criteria are met:
    - Control of the dummy identifier must remain with the Mountain Dental and must not be disclosed
    - The dummy identifier cannot be derived from individually identifiable information such as a Social Security number

Marketing

Policy: PHI will be used or disclosed for marketing purposes only as specified in the process outlined below. Note: Marketing activities that do not involve uses or disclosures of PHI are not subject to HIPAA privacy regulations.

Purpose: To be in compliance with the Privacy Rule.

Process:

- Mountain Dental must obtain a HIPAA-compliant authorization for uses and disclosures of PHI for marketing purposes.
- "Marketing" is defined by HIPAA as making a communication about a product or service that encourages the recipient of the communication to purchase or use the product or service (with the exception of the communications listed below), or an arrangement between the Mountain Dental and any other covered entity where the Mountain Dental discloses PHI in exchange for direct or indirect payment so that the other covered entity can make a communication about its own product or service that encourages the recipient of the communication to use or purchase that product or service.
- The following communications are specifically excepted from the definition of "marketing," so long as Mountain Dental does not receive financial remuneration in exchange for making the communication:
    - Communication for treatment, including case management or care coordination, or to direct or recommend alternative treatments, therapies, providers or settings of care; or
    - Communication to describe a health-related product or service provided by Mountain Dental;
- In addition, the following are NOT considered "marketing":
    - Face-to-face communications with the patient by Mountain Dental, its providers and/or workforce
    - Promotional gifts of a nominal value given to the patient by Mountain Dental, its providers and/or workforce.
    - Refill reminders or other communications about a drug or biologic currently being prescribed for the patient, so long as any financial remuneration received by Mountain Dental for making the communication is reasonably related to Mountain Dental's cost of making the communication.
- Authorizations for marketing communications for which Mountain Dental receives financial remuneration must include a statement to that effect.

Fundraising

Policy: PHI will be disclosed for fundraising purposes only as specified in the process outlined below.

Purpose: To be in compliance with the Privacy Rule.

Process:

- "Fundraising" is a communication to an individual by Mountain Dental, Mountain Dental's foundation or Mountain Dental's business associate for the purposes of raising funds for Mountain Dental.
- Certain PHI (described below) may be used by Mountain Dental, or disclosed to Mountain Dental's business associate or institutionally related foundation, for fundraising purposes without obtaining a HIPAA-compliant authorization from the patient:
    - Demographic information (name, address, other contact information, age, gender and date of birth;
    - Dates of health care provided to an individual;
    - Department of service information;
    - Treating physician
    - Outcome information; and
    - Health insurance status.
- In order to use the information listed above for fundraising purposes, Mountain Dental's Notice of Privacy Practices must include a statement that Mountain Dental may contact the patient for fundraising purposes and that the patient has a right to opt-out of receiving such communications.
- When the above-listed PHI is used for fundraising purposes, each fundraising communication must include a clear and conspicuous opportunity to opt out of future fundraising communications. The method of opting-out may not be unduly burdensome or involve more than a nominal cost (e.g., requiring an individual to write a letter is too burdensome; requiring the individual to return a pre-printed, pre-paid postcard is not).
- Employees will remove the names of patients who opt out from mailing lists and ensure they do not receive further fundraising communications.

Disclosures after death

Policy: Mountain Dental will continue to protect a patient's PHI for a period of 50 years after the patient's death, in accordance with all applicable HIPAA provisions.

Purpose: To ensure that a patient's PHI is protected after death as required by HIPAA.

Process:

- A patient is entitled to protection of his or her PHI up to 50 years after the date of death.
- Mountain Dental may use and disclose PHI on decedents in the same way, and subject to the same limitations, as it did prior to the patient's death, but may also make two limited additional disclosures:
    - Mountain Dental may disclose PHI to a coroner or medical examiner for identification purposes, determining a cause of death, or other duties authorized by state law.
    - Mountain Dental may disclose PHI to a funeral director, consistent with state law, as necessary to carry out duties with respect to the decedent. (If necessary, information can be released prior to and in anticipation of the death of a patient to a funeral director.)
    - Mountain Dental may disclose to a family member, other relative, close personal friend or any other person identified by the patient before death who was involved in the patient's care or payment for health care prior to the patient's death, PHI that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the patient that is known to Mountain Dental.
- After a patient's death, the patient's personal representative may act to authorize use and disclosure of his or her information. Whether a person is the patient's personal representative will depend on state law.
- Information on a decedent may be used for research purposes without authorization (if permitted by state law) if the Mountain Dental obtains from the researcher a representation that the information is solely for research on the PHI of decedents, documentation of the death of the individual, and a representation that the PHI is necessary for the research purposes.

Workers' compensation

Policy: PHI will be used and disclosed for workers' compensation purposes in accordance with state law.

Purpose: To ensure that state laws are followed with respect to workers' compensation disclosures.

Process:

- State law and/or federal law will be followed for issues regarding disclosures of PHI for workers compensation purposes.
- HIPAA permits disclosures of PHI that are authorized by state laws relating to workers' compensation or other similar programs that provide benefits for work-related injuries without regard to fault.
- Disclosures may be made to the extent permitted by state law. For example, state law may require disclosure of only that PHI that is directly relevant to the claim.

Sale of PHI

Policy: Mountain Dental will not sell PHI except as permitted by HIPAA.

Purpose: To prohibit the improper sale of PHI.

Process:

- Mountain Dental shall not sell PHI unless it obtains a HIPAA-compliant authorization from the patients who are the subject the PHI being sold. The authorization must include a statement that Mountain Dental is receiving remuneration in exchange for the PHI.
- A "sale of PHI" is defined as a disclosure of PHI by Mountain Dental, or a business associate of Mountain Dental, if applicable, where Mountain Dental or its business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.
- A "sale of PHI" does NOT include a disclosure of PHI:
    - For public health purposes;
    - For research purposes, where the only remuneration received by Mountain Dental or its business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI;
    - For treatment and payment purposes;
    - For the sale, transfer, merger or consolidation of all or part of Mountain Dental and for related due diligence;
    - To or by a business associate for activities that the business associate undertakes on behalf of Mountain Dental, and the only remuneration provided is by Mountain Dental to the business associate;
    - To the patient, when requested by the patient; or
    - For any other purpose permitted by the Privacy Rule where the only remuneration received by Mountain Dental or its business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose, or a fee otherwise expressly permitted by law.

Student immunizations

Policy: Mountain Dental will not disclose student immunization data except as permitted by HIPAA or state law.

Purpose: To disclose student immunization PHI to schools at the request of patients in a manner that is consistent with HIPAA.

Process:

- Mountain Dental may disclose student immunization PHI about a patient who is a student (or prospective student) to a school if all of the following are met:
    - The PHI that is disclosed is limited to proof of immunization;
    - The school is required by state or other law to have such proof of immunization prior to admitting the patient; and
    - Mountain Dental obtains and documents agreement to the disclosure from either (i) a parent, guardian or other person acting *in loco parentis* of the patient OR (ii) the patient, if the patient is an adult or emancipated minor.

Psychotherapy notes

Policy: Mountain Dental will use and disclose psychotherapy notes only as permitted by HIPAA and state law.

Purpose: To ensure psychotherapy notes are used and disclosed in compliance with HIPAA and state law.

Definition: "Psychotherapy notes" means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Process:

- Mountain Dental must have a HIPAA-compliant authorization to use or disclose psychotherapy notes, except:
    - To carry out the following treatment, payment or health care operations:
        - Use by the originator of the psychotherapy notes for treatment;
        - Use or disclosure by Mountain Dental for its own training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint family or individual counseling; or
    - When using or disclosing as required by law;
    - When using or disclosing for health oversight activities;
    - When disclosing to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law; or
    - When using or disclosing to prevent or lessen a serious threat to health or safety in certain circumstances, consistent with applicable law and standards.

Business Associates

HIPAA permits Entity to disclose PHI to business associates so that the business associate may assist Entity in performing a particular activity. The Privacy Rule requires that Entity execute a business associate agreement with all of its business associates prior to disclosing PHI to that business associate. This section covers the following:

1. Business associate agreements
2. Business associate relationship

Business associate agreements

Policy: PHI will not be disclosed to business associates of Mountain Dental unless a current and valid business associate agreement is in place, or unless otherwise permitted or required by law.

Purpose: To ensure that business associates of Mountain Dental understand Mountain Dental's privacy policies and agree to take reasonable steps to maintain the confidentiality of PHI that they may have access to in the course of doing business on behalf of Mountain Dental.

Definition:

- A "business associate" is a person or covered Mountain Dental who, on behalf of Mountain Dental, but other than in the capacity of a member of the workforce of Mountain Dental, creates, receives, maintains, or transmits PHI for a function or activity regulated by the Privacy and/or Security Rules, including but not limited to: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. § 3.20, billing, benefit management practice management and repricing; OR
- Provides, other than in the capacity of a member of Mountain Dental's workforce, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for Mountain Dental, where the provision of the service involves the disclosure of PHI from Mountain Dental or from a business associate of Mountain Dental; OR
- A Health Information Organization, E-prescribing Gateway or other person that provides data transmission services with respect to PHI to Mountain Dental and that requires access on a routine basis to such PHI; OR
- A person or covered Mountain Dental that offers a personal health record to one or more individuals on behalf of Mountain Dental; OR
- A subcontractor that creates, receives, maintains or transmits PHI on behalf of the business associate.
- A business associate does NOT include a health care provider with respect to disclosures by Mountain Dental to the health care provider concerning the treatment of an individual.

Process:

- It is the responsibility of Privacy Officer and/or Security Officer at MDSC to determine which persons or entities are "business associates" of Mountain Dental.
- Mountain Dental will execute a valid business associate agreement with each business associate prior to permitting the business associate to access, use or

disclose PHI and at all times during the term of the contract with the business associate.

- All business associate agreements are to be reviewed by the Security Officer at the Support Center to ensure that they meet the requirements of the Privacy Rule.
- Any employee who knows or suspects that a business associate is misusing PHI, not taking reasonable steps to safeguard the confidentiality of PHI or otherwise engaging in an activity or practices that would constitute a breach of the business associate agreement should notify the Privacy Officer or designee immediately.
- The Privacy Officer or designee will inform its business associates of any restrictions on the use or disclosure of PHI that Mountain Dental agrees to that affect the business associate's use of the information.

Business associate relationship

Policy: Mountain Dental will be conscious of the activities of its business associates and will take action when it knows that the business associate has violated HIPAA and/or the business associate agreement

Purpose: To ensure that business associate fulfills its responsibilities on behalf of Mountain Dental.

Process:

- If Mountain Dental knows of a pattern or activity or practice of a business associate that constitutes a material breach of the business associate agreement and/or HIPAA, Mountain Dental will take steps to correct the problem or, if such steps are unsuccessful, terminate the arrangement.
- If any Mountain Dental employee becomes aware of a potential problem, he or she should notify the Privacy Officer. The Privacy Officer should notify any other Mountain Dental personnel who may be able to assist with the situation, and should take reasonable steps to correct the problem.
- Mountain Dental personnel will contact the business associate as soon as possible after discovering the potential infraction to address the issue. Depending on the terms of the business associate agreement with the business associate, Mountain Dental will assess the options for termination or allowing a cure period.

Breach Notification Policies and Procedures

1. Identifying a breach of unsecured protected health information
2. Notification of breach to the individual(s)
3. Notification of breach to the media
4. Notification of breach to the Secretary

Identifying a breach of unsecured protected health information

Policy: Mountain Dental will identify all breaches of unsecured protected health information ("PHI") as defined in 45 C.F.R. § 164.402 in order to notify the appropriate parties.

Definitions:

"Breach" is the acquisition, access, use or disclosure of unsecured PHI that is not permitted by the Privacy Rule that compromises the security or privacy of the PHI.

Uses or disclosures that do **not** constitute a breach:

- An unintentional acquisition, access or use of unsecured PHI by a member of Mountain Dental's workforce, a person acting under the authority of Mountain Dental or one of Mountain Dental's business associates that (i) was made in good faith and within the scope of authority and (ii) does not result in further use or disclosure in a manner prohibited by the Privacy Rule.
- An inadvertent disclosure by a person who is authorized to access PHI at Mountain Dental to another person authorized to access PHI at Mountain Dental, or by a person authorized to access PHI at one of Mountain Dental's business associates to another authorized person at the business associate, if the information received is not further used or disclosed in a manner prohibited by the Privacy Rule.
- A disclosure of PHI where Mountain Dental or one of Mountain Dental's business associates has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

"Unsecured PHI" means PHI that Mountain Dental has not rendered unusable, unreadable, or indecipherable to unauthorized persons by through the use of a technology or methodology specified by the Secretary of HHS (which includes but is not limited to encryption).

Process:

- Mountain Dental will determine whether there has been an acquisition, access, use or disclosure of unsecured PHI that is not permitted by the Privacy Rule.
- Any such acquisition, access, use or disclosure of unsecured PHI that is not permitted by the Privacy Rule will be presumed to be a "breach" requiring notification under these policies, UNLESS Mountain Dental can demonstrate that there is a low probability that the PHI has been compromised based on an objective risk assessment of at least the following factors:
- The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;

    - E.g., financial information and social security numbers increases the risk of ID theft and financial fraud.
    - E.g., list of patient names, addresses and hospital ID numbers (easily re-identified) versus list of patient discharge dates and diagnoses (not as easily re-identified).
- The unauthorized person who used the PHI or to whom the disclosure was made;
    - E.g., disclosure to another covered Mountain Dental obligated to abide by the Privacy and Security Rules may lower the probability of the PHI being compromised.
- Whether the PHI was actually acquired or viewed; and
    - E.g., whether forensic analysis reveals that the PHI on the laptop stolen and later recovered was not accessed, viewed, acquired, transferred or otherwise compromised.
- The extent to which the risk to the PHI has been mitigated.
    - E.g., Mountain Dental may be able to obtain and rely on the assurances of another covered Mountain Dental that it destroyed the information it received in error.
- Mountain Dental will notify Mountain Dental's attorney if Mountain Dental is unsure of (i) whether there has been an acquisition, access, use or disclosure of unsecured PHI that is prohibited by the Privacy Rule, and/or (ii) whether there is a low probability that the PHI has been compromised.
- If Mountain Dental demonstrates that there is a low probability that the PHI has been compromised, Mountain Dental will document its risk assessment and conclusion, conduct appropriate mitigation procedures and take steps to ensure that a similar use or disclosure does not occur in the future.
- If Mountain Dental determines the acquisition, access, use or disclosure of PHI that is prohibited by the Privacy Rule does constitute a breach, Mountain Dental will refer to and follow the procedures for breach notification in the sections titled "Notification to the individual(s)," "Notification to the media," and "Notification to the Secretary."

Notification of breach to individual(s)

Policy: Mountain Dental will notify each individual whose unsecured protected health information ("PHI") has been, or is reasonably believed by Mountain Dental to have been, accessed, acquired, used or disclosed as a result of a breach by Mountain Dental or one of its business associates, in accordance with the procedures for notifying individuals at 45 C.F.R. § 164.404.

Definitions:

"Agent" shall mean any person or covered Mountain Dental that is authorized to act on behalf of Mountain Dental, including but not limited to Mountain Dental's directors, officers, contractors, subcontractors, service providers, and the employees, directors and officers of Mountain Dental's contractors, subcontractors and service providers.

Process:

- Mountain Dental will notify the individual in writing of the breach without unreasonable delay, and in no case later than 60 days after the date of discovery of the breach.
- The date of discovery of the breach is the first day that Mountain Dental knew about the breach, or would have known about the breach if Mountain Dental had exercised reasonable diligence in implementing effective internal policies for discovering breaches of unsecured PHI.
    - If any employee or agent of Mountain Dental (besides the person who committed the breach) knew of the breach, then the date of discovery is the date the employee or agent learned of the breach.
- Mountain Dental will contact Mountain Dental's attorney if Mountain Dental is unsure of (i) the date of discovery of the breach or (ii) whether an individual or Mountain Dental who caused the breach is an employee or agent of Mountain Dental.
- The notice to the individual (whether in written or substitute form, as described below) will include the following elements, to the extent possible:
    - A brief description of what happened, including the date of discovery of the breach, if known;
    - A description of the types of unsecured PHI that were involved in the breach (such as whether the individual's full name, social security number, date of birth, home address, diagnosis, disability code, or other types of information were involved);
    - Any steps the individual should take to protect the individual from potential harm resulting from the breach;
    - A brief description of what Mountain Dental is doing to investigate the breach, mitigate harm to individuals, and protect against any further breaches; and

    - Contact procedures for the individual to ask questions or learn additional information, which will include a toll-free telephone number, e-mail address, website or postal address.

- Mountain Dental will use the *Sample Notification Letter* to Individuals as a guide for drafting the notification.
- Mountain Dental will send the written notification by first-class mail to the individual at the last known address of the individual, or to the individual's email address, if the individual has previously agreed to electronic notice.
- If the individual is deceased, Mountain Dental will send the written notification to the next of kin or personal representative of the individual, if Mountain Dental has contact information for the next of kin or personal representative.
- If the individual's contact information is unavailable or out-of-date such that the individual is unreachable by mail, Mountain Dental will use a substitute form of notice that Mountain Dental believes will reach the individual.
    - If there are fewer than ten individuals who cannot be reached by mailed written notice, Mountain Dental will use an alternative form of notice, such as e-mail, telephone or other means.
    - If there are 10 or more individuals who cannot be reached by mailed written notice, Mountain Dental will post the notice conspicuously on the home page of Mountain Dental's website, or in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The notice will be posted for at least 90 consecutive days, and will include a toll-free phone number that remains active for at least 90 days, which an individual can call to learn whether the individual's unsecured PHI may be involved in the breach.
- If there is a possibility that the breach may cause imminent misuse of unsecured PHI, Mountain Dental will immediately notify the individual(s) by telephone or other appropriate means, in addition to the written notification described above.
- In addition to notifying the individual, Mountain Dental will notify the Secretary of the breach in accordance with the policy titled "Notification to the Secretary."
- If the breach involves more than 500 residents of any one state, county or city, Mountain Dental will notify the media in accordance with the policy titled "Notification to the media."

Notification of breach to the media

Policy: Mountain Dental will provide notification to the media as required by 45 C.F.R. § 164.406 if a breach of unsecured PHI involves more than 500 residents of one state, county or city.

Definitions:

"Prominent media outlets" shall mean the general interest newspaper(s), television station(s) and/or radio station(s) serving the state, county or city on a daily basis (or on the most frequent basis).

Process:

- Mountain Dental will provide notice of a breach involving 500 or more individuals in any one state, county or city to the prominent media outlets for that state, county or city. The prominent media outlets for a city would be the major television stations, newspapers and radio stations serving the residents of that city. If the 500 or more residents live across the entire state, the prominent media outlets notified must serve the entire state.
- Mountain Dental will provide the notice to the media without reasonable delay and in no case later than 60 calendar days after the date of discovery of the breach (see policy titled "Notification to the individual" to determine the date of discovery of the breach).
- The notice to the media will include the same information that is required for the written notification to the individual. The notice may be in the form of a press release. Mountain Dental will use the Sample Media Notification form as a guide.
- In addition to the notice to the media, Mountain Dental will provide notification of the breach to each individual in accordance with the policy titled "Notification to the individual" and notification to the Secretary in accordance with the policy titled "Notification to the Secretary."

Notification of breach to the Secretary

Policy: Mountain Dental will provide notification of all breaches of unsecured PHI to the Secretary of Health and Human Services (the "Secretary") as required by 45 C.F.R. § 164.408.

Process:

- Mountain Dental shall maintain a log of all breaches of unsecured PHI involving less than 500 individuals.
- The log shall include the following information regarding each breach to the extent possible:
    - Date of the breach;
    - Date of discovery of the breach;
    - Approximate number of individuals affected by the breach;
    - Type of breach;
    - Location of the breached PHI;
    - Type of PHI involved in the breach;
    - Brief description of the breach;
    - Safeguards in place prior to the breach;
    - Dates the individual notice was provided;
    - Whether substitute notice was required;
    - Whether media notice was required; and
    - Actions taken in response to the breach.
- Within 60 days of the end of the calendar year in which the breaches occurred, Mountain Dental shall submit electronically a breach notification form for each breach on the Secretary's website: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.
- If a breach affects 500 or more individuals, Mountain Dental will submit electronically a breach notification form at the Secretary's website at the same time that Mountain Dental notifies the affected individuals: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

Employment and Training Issues

HIPAA provides flexibility regarding most areas of employee training and discipline relating to the use and disclosure of PHI. There are certain general guidelines that covered entities must follow, however, and there are some particular areas of concern where covered entities must exercise particular caution. This section covers the following areas:

1. Training of employees
2. Discipline and mitigation for violations
3. Employee health records
4. Whistleblowers and workforce member crime victims

Training of Employees

Policy: All Mountain Dental employees will receive initial training on Mountain Dental's privacy policies and will be retrained when changes are made to existing HIPAA requirements or Mountain Dental's policies, according to the process as outlined below.

Purpose: To ensure compliance with HIPAA by all members of the workforce.

Process:

- New employees hired will receive training during their orientation to Mountain Dental and their job duties.
- Training updates must be provided whenever HIPAA and/or Mountain Dental's privacy and security policies and procedures change, within 90 days of the effective date of the changes, for all employees whose job responsibilities will be affected by the changes.
- If an employee's job function changes and the change affects the Employee's use or disclosure of PHI, appropriate training in privacy policies and procedures will be provided to the Employee related to the new job function.
- Mountain Dental will keep documentation of all employee training provided for at least the six years required by HIPAA.

Discipline and mitigation for violations

Policy: Appropriate sanctions will be applied for any employees who are in violation of Mountain Dental's privacy policies.

Purpose: To be in compliance with HIPAA's requirement of applying sanctions to employees who violate HIPAA and/or Mountain Dental's policies and procedures.

Process:

- A breach of confidentiality occurs when an employee violates Mountain Dental's privacy policies and procedures. Health records are highly confidential and must be treated with great respect and care by any individual with access to this information. An employee who breaches Mountain Dental's privacy policies and procedures is subject to formal disciplinary action, up to and including termination, as set forth in this policy and in Mountain Dental's other policies and procedures regarding disciplinary actions.
- Examples of breaches of confidentiality include (but are NOT LIMITED TO) the following:
    - Leaving a copy of patient medical information in a public area;
    - Leaving a computer unattended in an accessible area with health record information unsecured;
    - Accessing or reviewing birth dates or addresses of friends or relatives, or requesting that another individual do so, without a permissible purpose (permissible purposes are those that are explicitly authorized by Mountain Dental in these policies);
    - Accessing or reviewing ANY patient's record for any reason, or requesting that another individual do so, without a permissible purpose (permissible purposes are those that are explicitly authorized by Mountain Dental in these policies);
    - Accessing or reviewing confidential information of another employee that is also a Mountain Dental patient, without a permissible purpose (permissible purposes are those that are explicitly authorized by Mountain Dental in these policies); OR
    - Failing to comply with the requirements relating to technical security, including the use of passwords, access to databases, and logging out of the system.
- In the event of an employee's violation of Mountain Dental's policies regarding PHI and/or violation by an employee of the Privacy Rule, the nature of the sanctions will be determined by the Privacy Officer, with guidance from the Human Resources Department and the Operations team, in accordance with Mountain Dental's usual policies and procedures for disciplinary action.*

  **May wish to seek counsel from an employment attorney*

- Privacy Officer will maintain documentation of all sanctions applied. Documentation will also be placed in the employee's personnel file in the Human Resources Department at the Support Center.

Employee health records

Policy: Mountain Dental will use and disclose employee PHI only as specified in the process outlined below.

Purpose: To be in compliance with HIPAA and all applicable State and Federal employment laws.

Process:

- PHI of employees that is maintained by Mountain Dental in its capacity as a health care provider is subject to the same policies and procedures for uses and disclosures as is the PHI of other patients.
- PHI of employees that is included in employment records and maintained by Mountain Dental in its capacity as an employer is excluded from the definition of PHI under HIPAA and not subject to the policies and procedures related to protecting the privacy of PHI (even though some or all of the PHI may be the same as is maintained by Entity as a health care provider). Such information may include medical information needed to carry out employer obligations (e.g., FMLA, ADA, sick leave). Although not subject to the Privacy Rule, the information may be subject to other laws and regulations applicable to the disclosure of information in employment records.

Whistleblowers and workforce member crime victims

Policy: Mountain Dental employees will not be prevented from or disciplined for reporting violations of HIPAA

Purpose: To be in compliance with HIPAA and to promote internal compliance.

Process:

- A member of Mountain Dental's workforce may disclose PHI for "whistleblower" purposes, without violating HIPAA or Mountain Dental's policies, if the workforce member:
    - Believes in good faith that the covered Mountain Dental has engaged in conduct that is unlawful or violates professional or clinical standards, or that the care, services, or conditions at Mountain Dental potentially endangers one or more patients, workers, or the public; and
    - Makes the disclosure to either (i) a health oversight agency or public health authority authorized by law to investigate or oversee the covered Mountain Dental's care, or an appropriate accreditation agency to report failure to meet standards to Mountain Dental's misconduct; or (ii) an attorney retained by or on behalf of the workforce member for purposes of determining the legal options available to the workforce member regarding the conduct in question.
    - Mountain Dental employees may, if they choose to do so, report first to the Privacy Officer.
- If a workforce member is a victim of a crime, he or she must notify the Privacy Officer prior to making any disclosure to law enforcement officials. The following limited information may be disclosed by the workforce member with the approval of the Privacy Officer:
    - The PHI disclosed is about the suspected perpetrator of the crime; and
    - The PHI disclosed is limited to name and address; date and place of birth; social security number; ABO blood type and rh factor; type of injury; date and time of treatment; date and time of death; and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, facial hair, scars, and tattoos.

Physical and Electronic Handling of PHI

Protected health information (or "PHI") is defined as any of the information below that is maintained or transmitted in any form or medium, including electronic media):

- Information that is created or received by Mountain Dental relating to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to the individual and that identifies the individual or can be used to identify the individual.

All protected health information, or "PHI," must be handled appropriately by Mountain Dental at all times. This includes Mountain Dental's first handling of the information, its retention of information, its practices with sending and retrieving information, and its destruction of information when the PHI no longer needs to be retained. This section covers the following areas:

1. Storage and document retention
2. Disposal of documents
3. Email, regular mail, fax, voicemail, and telephone messages
4. Computer passwords, access, and other security

Storage and document retention

Policy: Mountain Dental will use its best efforts to ensure that documents and other information that is considered PHI is properly maintained and stored.

Purpose: To ensure that Mountain Dental has reasonable safeguards, policies, and procedures for the storage and retention of documents.

Process:

- As with many other areas of the regulations, HIPAA provides Entity with flexibility in the storage and retention of documents. There are, however, some guidelines that must be followed.
- On-site storage. Any health records or other forms of PHI that are stored on-site at Mountain Dental will be protected from unauthorized use, disclosure, or access. Mountain Dental will take reasonable steps to ensure that there is no authorized access to the information. This may include locking storage rooms and filing areas, not permitting unauthorized personnel or visitors into any area where records are stored, and/or requiring passcode or badge access to areas where records are stored. If any Mountain Dental personnel are aware of improprieties related to the storage of documents on-site, the Privacy Officer will be notified immediately.
- Off-site storage. If Mountain Dental maintains records off-site, it will ensure that the storage facility is secure, that there is no access to the records by any unauthorized persons, and that retrieval of documents is handled appropriately. Mountain Dental will enter into a Business Associate Agreement with any off-site storage and/or retrieval company, whether the storage is physical or electronic. If any Mountain Dental personnel are aware of improprieties related to the storage of documents off-site, the Privacy Officer will be notified immediately.
- Document retention. HIPAA requires Entity to retain the following documents for at least six (6) years following the date of the document's creation or the date it was last in effect (whichever is later):
    - Internal policies and procedures related to the use and disclosure of PHI
    - Communications related to PHI (e.g., requests for amendment of records)
    - Documents related to any other activities required by HIPAA (e.g., training logs)
    - Records of certain disclosures for purposes of accounting if the patient asks for an accounting.

The documents above may be retained in either written or electronic format.

Retention for medical records and other documents are not specifically addressed by HIPAA, and is mainly a matter of state law, other federal laws, and general risk management. Documents will be retained by Entity for, at a minimum, the length of time required by state or federal law for the type of records in question. Questions about retention of documents not specifically addressed in this policy (including billing records,

tax filings, and other business documents) should be addressed to the administrator and/or legal counsel.

Disposal of documents

Policy: Mountain Dental will dispose of PHI in an appropriate manner so that PHI is not unintentionally disclosed.

Purpose: To ensure the confidentiality of information no longer needed by Mountain Dental.

Process:

- Electronic media. Mountain Dental will dispose of electronic media containing PHI in accordance with the guidance issued by the U.S. Department of Health and Human Services ("HHS"), available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html. Mountain Dental must clear or purge all confidential information, including PHI, on any electronic storage media/device in accordance with the HHS guidance prior to the removal or sale of such devices.
- Paper, film or other hard copy media. Mountain Dental will dispose of any paper, film or other hard copy media containing PHI by shredding or destroying it such that it cannot be read or otherwise reconstructed. Mountain Dental will enter into a Business Associate Agreement with any third-party shredding or destruction company, if such company's duties involve destruction of Mountain Dental's hard copy media that contains PHI.
- Documentation of records destruction. Mountain Dental will appropriately document destruction of electronic and hard copy media containing PHI.

Email, regular mail, fax, voicemail, and phone messages

Policy: Mountain Dental will ensure that its communications by email, regular mail, fax, voicemail, and other messages will be reasonably limited in their use and disclosure of PHI.

Purpose: To ensure that PHI is not inappropriately disclosed by Mountain Dental.

Process:

- Email. Mountain Dental may communicate with patients via encrypted email if appropriate and if the patient consents to such communication (either in writing or orally, followed by documentation). If Mountain Dental communicates with a patient using unencrypted email, Mountain Dental must first notify the patient that there may be some level of risk that the PHI in the unencrypted email could be read by a third party. Mountain Dental personnel must ensure that the patient's email address is correct and that PHI is not inappropriately sent to third parties.
- Telephone messages. Mountain Dental may leave information on a voicemail system, answering machine, or with a person who answers the phone at a number provided by the patient. The information should be limited to the minimum amount necessary. In most cases, it is not be appropriate to leave medical information. Mountain Dental personnel should verify with the patient how he or she prefers to receive information, or if it is acceptable to leave messages. If this is not possible, Mountain Dental personnel should use discretion, and should not disclose medical information.

Computer passwords, access, and other security

Policy: Mountain Dental shall ensure that its computer and electronic security processes are reasonable and compliant with HIPAA.

Purpose: To establish a standard for creation of passwords, protection of passwords, and other electronic security provisions.

Process:

- Mountain Dental employees who need access to electronic PHI on Mountain Dental databases to perform their job functions will be given password access to such databases.
- If an employee has reason to believe his or her password is compromised, the employee must notify the Security Officer immediately.
- Employees are not permitted to share their passwords or use another employee's account login and password in any circumstance.