HIPAA Policies and Procedures

Spring 2022

Table of Contents

Right to Accounting of Disclosures of PHI
Right to Request Amendment
Complaints
Specialized Uses & Disclosures
Research
Limited Data Sets
De-identification
Marketing
Fundraising
Disclosures After Death
Sale of PHI
Student Immunizations
Business Associates
Business Associate Agreements
Business Associate Relationships
Breach Notification Policies and Procedures
Identifying a Breach of Unsecured PHI
Notification to Individuals
Notification to the Media
Notification to the Secretary
Employment and Training Issues
Training of Employees

Discipline and Mitigation for Violations
Employee Medical Records
Whistleblowers and Workforce Member Crime Victims
Security Risk Assessments and Audits
Security Awareness and Risks Assessments Policy
Audit/Activity Review
Forms
List of Designated Record Sets
Certification of Destruction
Designation of Privacy Officer
Designation of Security Officer
Notice of Privacy Practices
Acknowledgment of Receipt of Notice of Privacy Practices
Authorization for Use or Disclosure of Patient Information
Verification of Identity
Request for Access
Request for Restricted Use or Disclosure
Request for Confidential Communications
Request for Accounting of Disclosures and Response
Accounting of Disclosures Checklist
Log of Disclosures of Patient Information
Request for Amendment of Records and Response

Denial of Request to Amend
Amendment Request Log
Complaint Log
Data Use Agreement
Authorization for Marketing
Business Associate Agreement
Breach Assessment
Breach Log
Sample Breach Notification Letter to Individuals
Sample Media Notification
HIPAA Training Sign-In Sheet

Forms are designated in green throughout the Policy.

General

Overview

These policies and procedures are designed to provide our office with an outline for how to handle HIPAA-related privacy and security issues.

What is HIPAA?

HIPAA stands for the "Health Insurance Portability and Accountability Act of 1996" and includes both the "HIPAA Standards for Privacy of Individually Identifiable Health Information" (the "Privacy Rule") and the "Health Information Technology for Economic and Clinical Health (HITECH) Act" (the "Security Rule"). Dental practices are HIPAA "Covered Entities" and need to comply with HIPAA (as well as applicable State) requirements.

In general, HIPAA addresses how patient healthcare and payment data is created, used, stored, and shared, and the circumstances in which such data can be disclosed without patient consent. The HIPAA Privacy Rule also provides patients with rights to access their own health information.

HIPAA is primarily concerned with the protection of patients' Protected Health Information ("PHI," including electronic PHI ("ePHI")), which consists of any of the following that could be used to identify an individual who is the subject of this information:

- Name (including initials);
- Address;
- Dates related to the individual (including birth date and treatment date);
- Telephone and fax numbers;
- Email addresses;
- Social Security Numbers;
- Medical or dental record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers (including license plate);

- Device identifiers and serial numbers;
- URLs;
- IP address numbers;
- Biometric identifiers such as finger and voice prints;
- Full face photograph; and
- Any other unique identifying number, characteristic, or code

We should seek out legal counsel and/or compliance consultants when we have questions about HIPAA or its practical implications.

Designated Record Sets

Policy: We will create and maintain a list of its designated record sets.

Form(s): **List of Designated Record Sets**

Definitions:

Designated Record Set: Includes records maintained by and for our office that are:

- Medical and billing records about individuals maintained by or for our office;
- Enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health plan; and
- Used by or for our office to make decisions about individuals.

Process:

- We shall create and maintain (for a period of six (6) years) a list of its designated records sets.

Limiting Use and Disclosure of Patient PHI

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

Process:

- We will identify all employees, practitioners, or contracted workers who need access to PHI to perform their assigned job duties. The Privacy Officer, on a periodic basis, will review the list of access authorizations for appropriateness.
- Practitioners, 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, our office and our employees will limit any use or disclosure of PHI to the minimum necessary required to perform assigned duties.
- When we request PHI from another covered entity, we should request only the minimum necessary information, except where such requirements do not apply, as described below.
- 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 purposes;
    - 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 our office'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 our policies;
- Disclosures made to the Secretary of Health and Human Services (the "Secretary") for compliance and enforcement of the Privacy Rule; and
- Disclosures required for compliance with the other HIPAA provisions.

- Voicemails: We may leave the 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 appropriate to leave medical information.
  - E.g., For appointment reminders, leave only the following information on voicemail:
    - The patient you are calling for
    - Your name
    - Name of practice from which you are calling (e.g., Dr. ___'s office]
    - That you are calling wit an appointment reminder
    - The phone number to call if the patient has questions
- Our 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, our personnel should use discretion, and should not disclose medical information.

Incidental Disclosures:

- "Incidental disclosures" are not considered violations of HIPAA or State law law. These are disclosures that occur as an incident to a use or disclosure

that is otherwise permitted or required by law, so long as we implement reasonable and appropriate safeguards to prevent such incidental disclosures such as computer passwords, speaking quietly about PHI in public areas, etc.

- If an employee needs to discuss a patient's PHI over the phone or with another person in the office and cannot reasonably do so without other people hearing, he or she should move to a private location.

- 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 must be assessed to determine whether a breach of PHI occurred. See "Breach Notification Policies and Procedures".

Storage and Retention of Documents and Media Containing PHI

Policy: We will use its best efforts to ensure that documents and other media that contain PHI are properly maintained and stored.

Process:

On-Site and Off-Site Storage:

- On-site storage. Any health records or other forms of PHI that are stored on-site at our office location will be protected from unauthorized use, disclosure, or access. We 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 of our personnel are aware of improprieties related to the storage of documents on-site, they should notify the Privacy Officer immediately.
- Off-site storage. If our office maintains records off-site, we 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. We will enter into a Business Associate Agreement ("BAA") with any off-site storage and/or retrieval company, whether the storage is physical or electronic.

  If any of our personnel are aware of improprieties related to the storage of documents off-site, they should notify the Privacy Officer immediately.

Retention Periods for Documents or Media Containing PHI:

- **Health records.** We will generally retain health records for at least 10 years after the date of the last encounter (or with respect to minors, 10 years from when the minor reaches the age of 18). The following types of health records shall be kept indefinitely:
    - health records relating to patients with implantable devices;
    - known vaccination reactions;
    - bloodborne pathogen exposures and birth disabilities;
    - health records relating to incompetent patients; and
    - advance directives.

- **HIPAA documentation**. We shall 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); and
    - 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.

Questions about retention of documents not specifically addressed in this policy (including billing records, tax filings, and other business documents) should be addressed to our office's legal counsel and/or compliance consultants.

Destruction of Documents and Media Containing PHI

Policy: We will destroy or dispose of PHI in accordance with Federal and State laws and in a manner that renders PHI inaccessible to others.

Form(s): **Certification of Destruction**

Process:

- All destruction/disposal of patient health information media will be done in accordance with federal and state laws and regulations and pursuant to our "Storage and Retention of Documents and Media Containing PHI" policy. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- Records involved in any open investigation, audit, or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
- Before reuse of any recordable and erasable media (i.e., hard disks, tapes, cartridges, USB drives, smartphones, SAN disks, SD, and similar cards), all ePHI must be rendered inaccessible, cleaned, or scrubbed. Standard approaches include one or all of the following methods:
    - Overwriting the data (for example, through software utilities); or
    - Degaussing (i.e. use a magnetic field to erase the data bits stored on magnetic) the media.
- Records scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of PHI is complete.
- Any BAA must provide that, upon the termination of the contract, the business associate will return or destroy/dispose of all patient health

information. If such return or destruction/disposal is not feasible, the contract must limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.

- We shall maintain a record of all PHI media sanitization. We have the responsibility to retain the burden of proof for any media destruction regardless of whether destruction is done by the organization or by a contractor. Retention is required because the records of destruction/disposal may become necessary to demonstrate that the patient information records were destroyed/disposed of in the regular course of business. Records of destruction/disposal, such as a certificate of destruction, should include:
    - Date of destruction/disposal;
    - Method of destruction/disposal;
    - Description of the destroyed/disposed of record series or medium;
    - Inclusive dates covered;
    - A statement that the patient information records were destroyed/disposed of in the normal course of business;
    - The signatures of the individuals supervising and witnessing the destruction/disposal.
- Copies of documents and images that contain PHI and are not originals that do not require retention based on retention policies (e.g., provider copies, schedule print-outs, etc.) shall be destroyed/disposed of by shredding or another acceptable manner as outlined in this policy. A certification of destruction is not required.
- If destruction/disposal services are contracted, the contract must provide that the organization's business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law. The BAA should also set minimum acceptable standards for the sanitization of media containing PHI. The BAA or contract should include but not be limited to the following:
    - Specify the method of destruction/disposal;
    - Specify the time that will elapse between acquisition and destruction/disposal of data/media;
    - Establish safeguards against unauthorized disclosures of PHI;
    - Indemnify the organization from loss due to unauthorized disclosure;

    - Require that the business associate maintain liability insurance in specified amounts at all times the contract is in effect; and
    - Provide proof of destruction/disposal (e.g., certificate of destruction).
- Any media containing PHI should be destroyed/disposed of using a method that ensures the PHI could not be recovered or reconstructed. Some appropriate methods for destroying/disposing of media are outlined in the following table:

Medium	Recommendation
Audiotapes	Recycling (tape over), degaussing, or pulverizing.
Electronic Data/ **Hard Disk Drives including drives found in printers or copiers**	Overwriting data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten.
Electronic Data/ Removable media or devices including USB drives or SD cards	Overwriting data with a series of characters or reformatting the tape (destroying everything on it). Total data destruction does not occur until the data has been overwritten. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Shredding or pulverization should be the final

	disposition of any removable media when it is no longer usable.
Handheld devices including cell phones, smartphones, PDAs, tablets, and similar devices.	Software is available to remotely wipe data from handheld devices. This should be standard practice. Any removable media that is used by these devices should be handled as specified in the previous paragraph. When a handheld device is no longer reusable it should be totally destroyed by recycling or by trash compacting.
Optical Media	Optical disks cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
Microfilm/ **Microfiche**	Recycling and pulverizing.
PHI Labeled Devices, Containers, Equipment, Etc.	Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Removing labels or incineration of the medium would be appropriate. Another option is to obliterate the information with a heavy permanent marker pen. Ribbons used to print labels may contain PHI and should be disposed of by shredding or incineration

Paper Records	Paper records should be destroyed/disposed of in a manner that leaves no possibility for the reconstruction of information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing. If shredded, use cross-cut shredders which produce particles that are 1 x 5 millimeters or smaller in size.
Videotapes	Recycling (tape over) or pulverizing.

The Privacy Officer should periodically reassess the appropriateness of methods of destruction, disposal, and reuse based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.

Workstation and Software Usage Policy

Policy: We will follow reasonable and prudent hardware and software practices for legitimate business purposes only, in order to prevent unauthorized access to our network (i.e., through virus attacks or infection to network systems) and to protect the security, integrity and reliability of electronic equipment.

This policy applies to all users of our office's computers and related equipment, including, but not limited to, cellular devices, PDA's, office phones, hand-held scanning devices, and copy/fax machines. Additionally, this policy applies to PHI on systems at a user's home office or any other location while connected by any cellular, dialup or broadband connection.

Process:

Monitoring and Enforcement:

- We reserve the right to monitor and/or inspect email accounts, personal file directories, web access, phones, and any information stored on the company computers and related equipment at any time without notice. All data and communications, included but not limited to emails, should be considered company property and are subject to audit at any time.
- We reserve the right to enforce this policy; violation of the policy by any employee will be subject to disciplinary action up to and including termination of employment; and in certain situations, legal or criminal prosecution.

Strictly Prohibited Use or Activities:

- The following activities are strictly prohibited. This list is not meant to be all-inclusive:

- Access, acquisition, storage, or dissemination of data which is illegal, pornographic, or which negatively depicts sex, race, religion, sexual orientation, marital status, military status, disability, national origin or any protected class.
- Use for conducting a personal business enterprise, political or religious activities, engaging in any form of intelligence review or collection of our office's data, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.
- Downloading or playing music, video games, copyrighted or patented materials, or any other data used for personal interests.
- Accessing outside personal email accounts or using personal email accounts to access any of our systems or networks.
- Accessing any gaming or gambling sites.
- Creation and/or administration of Web sites or blogs (unless specifically authorized).
- Participation in "chat rooms" or any social networks for any reason other than specific business related activities is prohibited on company time, i.e. Facebook, Twitter, etc.
- Inappropriate postings on social networks that disparage the company or any of its associates.
- Circulation of "chain emails"; emails that are disruptive, offensive or harmful to morale, ethnic slurs, racial comments, jokes, or anything construed as harassment or showing disrespect for fellow associates, customers, or vendors.
- Sending an email under the guise of another person.
- Unapproved access, altercation, destruction, or tampering with email or any document or other data.

Passwords:

- Passwords should be at least eight (8) characters in length and include a combination of letters and numbers.
- Passwords should be changed every three months.
- Passwords should not be shared with or disclosed to others.
- Employees should never use another employee's password.

- Employees should not post passwords on their workstations, desktops, under their desks or any other place that could be accessed by an unauthorized person.
- If an employee has reason to believe his or her password has been compromised, he or she must notify the Security Officer immediately.

Flash Drives:

- Flash drives must utilize password protection as provided by the device.
- Flash drives should be used as a means to transfer data from one machine to another. They should not be used to store critical data.

Remote Access:

- Connecting to our office's network is permitted only with devices and configurations approved by the Security Officer. All access must be done through secure password authentication.

Use of Email and the Internet:

- All employees have a responsibility to use email and the Internet in a professional, lawful, and ethical manner.
- Where no policy or guideline exists, employees should use good judgment and take the most prudent action possible. If uncertain about any issue, employees can consult with their supervisor.

Software Use Policy:

- All software loaded, downloaded, stored, or placed in any way into an office-owned computer, software resident device, or any other device utilized for business purposes must have a specific business use and be properly licensed, installed, and utilized.
- Any approved personal software may only be loaded, downloaded, stored, or placed in any way on an office-owned computer with the written approval of the Security Officer and subject to a copy of a valid software license being filed before any installation, access, or use.

- Further, all software loaded, downloaded, stored, or placed in any way into an office-owned computer shall be accessed, used or interfaced with other computer software only in strict compliance with the terms of such software license and applicable law.
- The Security Officer will periodically audit all computers and software resident devices to ensure compliance with this policy.
- Violation of this policy may be grounds for disciplinary action up to and including dismissal from employment.

Terminated Employees:

- Employees who leave the Practice, whether voluntarily or non-voluntarily, will cease to have access to our hardware and software.
- Prior to the employee's departure, the Security Officer will meet with the employee to reiterate our "Discipline and Mitigation for Violations" policy and explain that any unauthorized attempts to access patient PHI will be referred to appropriate authorities.

Encryption and Decryption Policy

Policy: We will implement policies and procedures to encrypt and decrypt ePHI.

Process:

- The Security Officer will be responsible for selecting and overseeing the installation of appropriate software to encrypt and decrypt ePHI.
- All ePHI in our office's systems and included in outbound communications (e.g., emails) must be encrypted.

Appointment and Duties of Privacy Officer

The Privacy Rule requires a Covered Entity to designate a Privacy Officer, who is responsible for creating and implementing the entity's privacy policies and practices.

Policy: Our office's Privacy Officer is responsible for developing and implementing privacy and breach notification policies and procedures.

Form(s): **Designation of Privacy Officer Form**

Process:

- We will document the designation of its Privacy Officer by having such person complete and sign the **Designation of Privacy Officer Form**.
    - Retain this documentation for at least six (6) years from the date of its creation or the date when last in effect, whichever is later.
- The Privacy Officer should be someone who is familiar with both the dental and administrative functions of the Practice and who has the organizational, problem solving and communication skills to research and implement applicable privacy regulations.

Appointment and Duties of Security Officer

The Security Rule requires a Covered Entity to designate a Security Officer, who is responsible for creating and implementing the entity's security policies and practices.

Policy: Our office's Security Officer is responsible for developing and implementing procedures to prevent, detect, contain and correct security violations.

Form(s): Designation of Security Officer Form

Key Definitions:

- Administrative Safeguards: actions, policies and procedures to manage security measures to protect ePHI and to manage the Practice's workforce in relation to the protection of that information.
- Information System: an interconnected set of information resources that normally includes hardware, software, information, data, applications, communications and people.
- Physical Safeguards: physical measures, policies and procedures to protect the Practice's or its Business Associates' electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.
- Security: encompasses all of the administrative, physical and technical safeguards in an information system.
- Technical Safeguards: the technology and the policies and procedures for its use that protect electronic protected health information and control access to it.

Process:

- We will document its designation of its Security Officer (who may, but is not required to be, the same person as the Privacy Officer) by having such person complete and sign the **Designation of Security Officer Form**.
    - Retain this documentation for at least six (6) years from the date of its creation or the date when last in effect, whichever is later.
- The Security Officer should be someone who is familiar with both the dental and administrative functions of the Practice and who has the organizational, problem solving and communication skills to research and implement applicable security regulations.

Notice and Acknowledgment of Privacy Practices

The Privacy Rule requires a Covered Entity to provide to its patients a description of the privacy practices.

Policy: We will provide a written notice to its patients of its uses and disclosures of PHI (the "NPP"). The NPP shall be in Plain English and describe patients' rights and our office's legal duties with respect to PHI.

Form(s): **Notice of Privacy Practices; Acknowledgment of Receipt of Notice of Privacy Practices Form**

Process:

Distributing the NPP:

- We will post the NPP in a prominent location in its office and on its website as well as make a good faith effort to provide a copy of the NPP to every patient with whom it has a direct treatment relationship *before or at the time of first service delivery*. See **Notice of Privacy Practices**.
    - If the patient presents in person for his/her first service delivery, we shall provide the NPP to the patient at that time (unless previously sent to the patient).
    - If the first service delivery to the patient is made by telephone or electronic mail, we shall mail a copy of the NPP (via regular or email, as applicable) on the day of the service delivery (unless previously sent to the patient).

Our office need only directly provide the NPP to each patient one time; subsequently, the NPP must be available to every patient upon request.

- Telephone contact with patients solely for the purpose of scheduling an appointment is not considered a "service delivery."
- Persons who receive a copy of the NPP via electronic mail are also entitled to receive a paper copy upon request.

Patient acknowledgment of Notice:

- We will make a good faith effort to obtain written acknowledgment from each patient that he/she has received a copy of the NPP. See "Acknowledgment of Receipt of Notice of Privacy Practices Form."
- If the patient refuses or is unable to acknowledge receipt of the copy of the NPP (or does not return a mailed copy of the NPP), the employee involved shall document the good faith effort to obtain acknowledgement and the reason that it was not obtained.
- The acknowledgement and/or documentation of the good faith effort must be retained according to the Practice's record retention policy (i.e., six (6) years).
- We may continue to treat the patient even though he or she has refused or is unable to acknowledge receipt of the NPP.
- In an emergency treatment situation, distribution of the NPP may be delayed until reasonably practicable after the emergency ends. There is no need to get an acknowledgement in emergency situations, even after the emergency ends.

Changes to the NPP:

- We reserve the right to change our NPP. The Privacy Officer will update the NPP and is responsible for posting to the website the revised NPP and educating staff, as appropriate.
- Updated NPPs do not have to be given to patients or others except upon request.
- We must provide a copy of the NPP to any individual who does not have a direct treatment relationship with us, if requested, but we need not obtain acknowledgement of receipt of the NPP from those individuals.

General Uses and Disclosures; Patients' Right to Request

Permitted Uses and Disclosures

Policy: We will use and disclose PHI only as permitted or required by HIPAA.

Process:

General rule: Except as noted below, we *must obtain written consent* of the patient (or his/her authorized representative) to use or disclose PHI or release medical records or medical information to any person outside of our practice. See "Patient Consent/Authorization Policy" immediately following for instructions on how to obtain consent.

Exceptions: NO WRITTEN CONSENT is required for disclosures to:

- The patient.
- The patient's personal representative (who has the right to make health care decisions for the patient) unless the Practice has reasonable belief that:
    - The patient has been or may be subject to domestic violence, abuse or neglect by the personal representative;
    - disclosure to the personal representative could endanger the patient; or
    - the Practice determines that it is not in the best interest to give information to the personal representative.

    NOTE: If the patient is deceased, it is OK to provide the patient's information to the patient's executor or estate administrator but the Practice should request proof of the patient's death and the legal status of the representative.
- The patient's family member, relative, close personal friend or other person who is involved in the patient's care or payment for care, if the information is relevant to the person's involvement.

- If the patient is present, PHI may be disclosed only 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, we 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 are met.

- To persons within our practice and to our business associates with whom we have entered into a business associate agreement, for purposes of treatment, payment, or 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 our activities to obtain or provide reimbursement for provision of health care.
  - Health care operations includes many of the activities necessary to operate our practice, including quality assurance and improvement, reviewing 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.
- Medical emergencies
  - No written consent required when we are unable to obtain the patient's consent due to the patient's condition or the nature of the emergency.
- Court orders
  - A patient's health record may be provided without patient consent in accordance with a proper court order. NOTE: neither a subpoena nor an attorney demand letter is a court order.
- Workers' compensation
  - A patient's health records reasonably related to the workers' compensation injury must be provided to the patient's (employee),

employer or employer's workers compensation insurer without patient consent.
    - Only records related to the work injury may be disclosed.
- Public health reporting
    - We must report positive cases of certain infectious diseases to the State Department of Health ("DH"). The DH may request further information on these cases for public health reasons, and a patient's release is not required. The DH will generally make these requests in writing, specifying the statutory authority.
- Child abuse (maltreatment of minors)
    - Health care professionals must report to a local welfare agency, police department or county sheriff within 24 hours if the professional knows or has reason to believe that a child has been neglected or physically or sexually abused. Oral reports must be followed by a written report within 72 hours.
    - We must help its health care professionals to comply with the mandatory reporting requirement and cooperate and provide information for investigations.
- Any other release authorized by law
    - There are a few other circumstances in which health records may be released to a government authority (court, CMS, DH, FDA, etc.). If someone asserts that they have legal authority to obtain a health record without the patient's consent, we should require the requesting party to provide us with a copy of the statute, rule, regulation or other authority. We should retain the authority in the patient's record. We should consult with legal counsel if there is a question of whether medical records may be disclosed.

Documentation of disclosures of PHI:

- We will document in the patient's medical record each use or disclosure of PHI except for the following disclosures:
    - to carry out treatment, payment or healthcare operations;

- to the patient or the patient's personal representative;
- incidental disclosures (except as a result of an error or neglect);
- pursuant to an authorization;
- to persons involved in the patient's care under HIPAA;
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials; or
- as part of a limited date set.

- The documentation will include the date of the disclosure and the circumstances under which the disclosure was made, the person or agency to whom the disclosure was made, and the records that were disclosed.

If you are unsure about whether you can use or provide patient information without the patient's consent, ask the Privacy Officer who will consult, as necessary with legal counsel or compliance consultants.

Patient Consent/Authorization

Policy: We will not use or disclose patient information without written consent unless such use or disclosure is permitted without consent or required by HIPAA.

Form(s): **Authorization for Use or Disclosure of Patient Information Form**

Process:

Contents of the written authorization:

- The authorization must be completed and must be signed by the patient, or the patient's personal representative. See **Authorization for Use or Disclosure of Patient Information Form**. We must verify that the person who signs the authorization has this authority.
- A valid authorization must be written in plain language and contain at least the following elements:
  1. Patient's name or other identifier(s);
  2. Name/identification of person or class of persons authorized to use or disclose the PHI;
  3. Name/identification of person or class of persons authorized to receive the PHI;
  4. Specific and meaningful description of the information being used or disclosed;
  5. Description of each purpose of the disclosure;
  6. Date and signature of the patient or personal representative and, if signed by a personal representative, the description of such person's authority to sign on behalf of the individual;

7. Expiration date of the authorization, or event that relates to the individual or the purpose of the use or disclosure which would cause the authorization to expire;
8. Statement of the individual's right to revoke (and the process for revoking) the authorization;
9. Statement of prohibition on conditioning treatment, payment, enrollment or eligibility for benefits on authorization, except in certain circumstances;
10. Statement that information disclosed to recipients who are not covered by HIPAA may be subject to re-disclosure by these recipients and no longer be protected by the HIPAA Privacy Rule;
11. For authorizations to use or disclose PHI for marketing purposes, if applicable: Statement that we received financial remuneration in exchange for making the marketing communication.
12. For authorizations to sell PHI, if applicable: Statement that we received direct or indirect remuneration in exchange for the sale.

ID and Authority Verification

Policy: We will not disclose patient information to persons who do not have the authority to access the information.

Form(s): **Verification of Identity Form**

Process:

- We will take reasonable steps to verify the ID and authority of individuals requesting PHI.
- Below is a list of typical requestors and how our employees may verify their identity:
    - Patient request**.** A patient is entitled to his/her own PHI. When requesting his/her own records, s/he should present a photo ID or other information you can use to identify them. Any other person requesting the patient's PHI must make the request in writing and get it signed and validated.
    - Public official or law office**.** To verify the *identity* of a public official, you must get a written statement of their identity on agency letterhead, an ID badge, or similar identifier, such as a .gov email address. To verify their *authority* to request PHI, they must present a written statement on agency letterhead stating the legal authority for requesting the release of information. Showing an ID badge and verbally stating the need for the request is insufficient. Note: Law enforcement is not typically entitled to PHI without a court order, warrant, or patient authorization. However, certain situations allow you to disclose PHI to law enforcement.
    - Requester acting on behalf of a government agency**.** Sometimes an organization will act on behalf of a government agency. In this case, you should examine documents supporting this claim, such as a contract or other official statement.

- Legally authorized representative**.** If a legally authorized representative of a patient makes a request, confirm that they are the patient's legal representative in the medical record. They may present a photo ID, a valid power of attorney for health care, court order, or other verification of their identity and authority as a representative.
- Request on behalf of a minor**.** A person making a request on behalf of a minor should present a birth certificate, power of attorney, letter of guardianship, court order, or other evidence of their relationship to the minor and/or their authority to act on the minor's behalf.

- We shall use the **Verification of Identity Form** to document that it has verified the identity of the person(s) requesting patient PHI.
- When in doubt, the Privacy Officer should handle all such requests and consult with legal counsel or compliance consultants as deemed necessary.

Minors

Policy: We will use and disclose the PHI of minors only as specified in the process outlined below. For purposes of this policy, a "minor" is an individual under the age of 18.

Process:

- 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.
- Divorced Parents. If the minor's parents are divorced, usually either parent may authorize treatment and the release or access of their child's medical records, regardless of which parent has physical custody of the child.

  Exception: If the parental rights of a parent have been legally terminated, or the parent's right to gain access to health care records have been legally restricted, that parent cannot authorize a release of, or gain access to, his or her child's medical records. If one parent asserts that the other parent may not have access or authorize treatment, we should request the parent to provide us with appropriate legal documentation of their assertion.

  - Adoptive Parents. Adoptive parents have the same rights as other parents to gain access and/or authorize the release of their child's health care information.
  - Legal Guardian/Conservator. If the minor patient has a legal guardian or conservator appointed by a court, the legal guardian or conservator may authorize a release of, or gain access to, a minor patient's medical records. The appointment papers should, however, be reviewed to verify the representative's authority.

- Situations where parents/legal guardians are not permitted by State law to access their minor children's health records:
    - Emancipated minors. A parent/legal guardian does not have access to a minor's health record if the minor is living separate and apart from his or her parents or legal guardian, whether with or without the consent of the parent or guardian, regardless of the duration of such separate residence and who is managing the minor's personal financial affairs.
    - Minor has married or borne a child. A parent/legal guardian does not have access to a minor's health record if the minor has been married or has borne a child. If the minor has borne a child, the parent/legal guardian of the minor does not have access to the child's medical records.
    - Pregnancy, VD, alcohol or drug abuse. A parent/legal guardian does not have access to a minor's health record relating to treatment for pregnancy and conditions associated therewith, venereal disease, or alcohol or other drug abuse, if the minor has consented to such treatment.
    - Hepatitis B Vaccination. A parent/legal guardian does not have access to a minor's health record relating to a Hepatitis B vaccination if the minor consented to the treatment.
- We may disclose PHI to the parent/legal guardian in any of the above situations where, in the judgment of a healthcare professional, failure to inform the parent/guardian would seriously jeopardize the minor's health.
- 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.

Right to Request Access to PHI

Policy: We will comply with a patient's request to access (i.e., see or get copies of) his or her own medical records, as specified in the process outlined below. It is the responsibility of the Privacy Officer to receive and process requests for access. If access is denied by us, patients may have the right to review the reason for denial.

Form(s): **Request for Access Form**

Process:

Written requirement:

- Patient requests for access to their own PHI must be in writing, signed by the patient, and must clearly identify the designated person and where to send the copy. Patients should use the **Request for Access Form** to request their own PHI.

Access to PHI may be denied* when:

- A health care professional at our office determines that the information is detrimental to the physical or mental health of the patient, or is likely to cause the patient to inflict harm to the patient or others.
  - If we deny access to the patient for this reason, we may supply the information to an appropriate third party or to another provider. The third party or other health care professional may release the information to the patient.
- When access is denied:
  - 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). Note: A patient does not have a right to review the grounds for denial when:
  - The PHI was compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding;
  - The PHI consists of certain clinical laboratory information; or
  - The PHI was obtained from someone other than our office under the promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
- The patient must also be given information on how to file a complaint to our office and appropriate contact information for the complaint process.
- When a 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 healthcare 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 14 business days after which the patient must be given written notice of the results of the review.
  - If access is denied, the patient has the right to review the denial of access.

*It's prudent to consult with outside counsel before denying a request.

Timeline for granting access:

- Written requests for access to PHI must be acted on within 30 days. If we are unable to comply within the 30 days, a one-time extension of an additional 30 days is allowed if we notify the patient in writing of the date by which it will comply with the request.

- If the PHI requested is not held by us, but we are aware where the PHI is held, the patient must be informed.

Format of PHI provided to patient:

- If a 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 a patient requests PHI in an electronic format, we must provide the PHI in the electronic format requested by the patient if we maintain 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, we 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).
- We may choose to provide a summary rather than the complete record if acceptable to the patient.
- We must transmit the PHI (whether paper or electronic) to a person or someone 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.

Fees:

- We 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. In no event may the

fee exceed that set by the State Department of Health for the current year. NOTE: There is a $10 duplication fee for patient requests.

- If the charge for a summary is extra, patients must be informed in advance and agree to the charge.

Restrictions on the Use or Disclosure of PHI

Policy: We will respond to a patient's request for restricted disclosure of PHI as outlined in the process below. [Name of Practice] is not required to comply with all such requests.

Form(s): **Request for Restricted Use or Disclosure**

Process:

Writing requirement:

- All requests by patients to restrict disclosure of PHI beyond what is required by law or otherwise noted in our policies must be in writing. Patients should use the **Request for Restricted Use or Disclosure Form** to request restrictions.

- Examples of such restriction requests would be:
    - requesting that PHI not be disclosed to an outside physician 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:

- We are not required to comply with all requests (i.e., those that may result in our inability to treat the patient or bill for services rendered).
    - One exception: We must comply with an individual's request to restrict the disclosure of PHI to a health 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 us out of pocket in full. We 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

we cannot unbundle the items or services, we should inform the patient and give the patient the option to restrict and pay out of pocket for the entire bundle. If we unbundle the services, we must counsel the patient on the consequences of doing so (i.e., the health plan may still be able to identify the services performed based on context).

- HMOs. If we are prohibited by law (not just contractually) from accepting payment from the patient above the cost-sharing amount, we may inform the patient that he/she must use an out-of-network provider in order to restrict disclosure to the HMO.

Process for reviewing requests:

- All requests for restricted disclosure will be processed by the Privacy Officer at the office level to ensure that the ability to treat the patient, bill for services rendered and otherwise perform necessary functions is not impeded by the requested restriction.
- If the Privacy Officer approves the request, the restrictions must be documented in the health record and appropriate staff must be notified.
- If the request for restricted disclosure is approved, we are bound by that agreement, unless the patient requests or agrees to the removal of the restriction in writing (or we document such oral agreement), or we terminate the restriction as provided below.

Denying requests for restriction:

- The Privacy Officer may not give approval to any restrictions of disclosure if the disclosure is required by court order, statute or other law.

Emergency situations:

- In the case of a medical emergency, when previously agreed upon restrictions on disclosure of PHI have been established, we may use the PHI as necessary to provide emergency treatment.

- If we disclose PHI to another provider in an emergency, we must request that the provider agrees not redisclose the PHI to others or use the PHI other than for the emergency.

Termination of restrictions:

- The patient may terminate the restrictions on the disclosure of PHI in writing or verbally (and if verbal, the agreement to terminate must be documented).
- Except as provided below, we may terminate a restriction after we notify 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 we terminate a restriction on disclosures to a health plan for payment or health care operations pertaining solely to an item or service for which a patient has paid us out of pocket in full.

Right to Request Confidential Communications

Policy: We will honor all reasonable requests made by a patient for alternative methods of communication (e.g., mail, voice message, different address or phone #, etc.).

Form(s): **Request for Confidential Communications Form**

Process:

Writing requirement:

- Requests for alternative methods of communication must be made in writing by the patient. Patients should use the **Request for Confidential Communications Form** to request confidential communications.

Reviewing requests:

- We may not inquire as to the reason for the request.
- If the request for alternative method(s) of communication affects our ability to collect payment for services, we should clarify with the patient how payments will be handled and note the same on the above-mentioned form.
- If the patient requests that we not use the patient's address on file, we should obtain an alternate address from the patient.
- If the patient does not clarify how payments will be handled or does not give an alternate address, we may refuse the request.
- All requests must be forwarded to the Business Office Manager for review.
- After review and approval by the 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 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.

Right to Accounting of Disclosures of PHI

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

Form(s): **Request for Accounting of Disclosures and Response Form; Accounting of Disclosures Checklist; Log of Disclosures of Patient Information**

Process:

Right to request accounting:

- Patients may request an accounting of disclosures by us and our business associates of their PHI for a specified period of time up to six (6) years prior to the date of the request (but not for disclosures made prior to April 14, 2003). Patients should use the **Request for Accounting of Disclosures and Response Form** to make such requests. Disclosures may be kept in the **Log of Disclosures of Patient Information**.
- The Business Office Manager, with assistance from the Privacy Officer, will be responsible for receiving and processing all requests for an accounting of PHI disclosures.
- We will use the **Accounting of Disclosures Checklist** to determine which disclosures must be included in the accounting to the patient. (See the subsection "Documentation of disclosures of PHI" under "Permitted Uses and Disclosures" herein)

Timeline for providing accounting:

- We must provide the accounting within 60 days of the request.

- A one-time extension of an additional 30 days will be allowed if the requestor is notified in writing as to the reason for the delay and the date by which the accounting will be provided.

Contents 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 the accounting for only the first disclosure must include the information noted above. However, the frequency and number of disclosures, date range of the accounting period and date of the last disclosure must be included.

- A "short cut" accounting is allowed 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 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, [Name of Practice] 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.
- If we decide to charge the patient for the additional accountings, we 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. Employees contacted by law enforcement must notify the Privacy Officer immediately.

Right to Request Amendment

Policy: Patients have the right to request amendment of their PHI and we will follow the process outlined below when considering the amendment request.

Form(s): **Request for Amendment of Records and Response Form; Denial of Request to Amend Form; Amendment Request Log.**

Process:

Writing requirement:

- The Privacy Officer is responsible for receiving and processing requests for amendments to health records.
- Requests for amendment of PHI must be made in writing and include the reason for the request. Patients should use the **Request for Amendment of Records and Response Form** to request health records.
- When making amendments, insert or append the new information and keep a record of the original information.

Timeframe for responding to request:

- We must respond to the request within 60 days from the date of receipt.
- A one-time extension of an additional 30 days will be allowed if the patient is notified 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:

- We have the right to refuse the amendment request under the following circumstances:

- The PHI requested was not originally created by us, unless the patient provides a reasonable basis to believe that we originally created the PHI is no longer available to take action on the request.
- The PHI requested is not included in the medical record held by us or is not part of a designated record set.
- The PHI requested is the type to which patients do not have the right to access (e.g., psychotherapy notes).
- The PHI requested is deemed to be accurate and complete.

- If the request for amendment is granted, the Privacy Officer, along with a healthcare professional, must make the amendment to the record.
- When amendment requests are granted, the patient must be notified and given the opportunity to identify persons that have received the PHI subject to the amendment.
- We must make a reasonable effort to provide the amended information to those identified by the patient as having the PHI that is subject to the amendment within 30 days.
- The amended information should also be provided to anyone (including business associates), with the patient's agreement, that is known by us to have the PHI that is subject to the amendment and that might rely on the unamended PHI in a manner that could be detrimental to the patient.
- Denials of amendment requests must be given to the patient within 60 days (unless we have 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 their disagreement with the denial in writing (and the process for submission);
  - The patient's right to request that we will include the original amendment request and the denial with any subsequent disclosure of the affected PHI; and
  - Information for the patient regarding how to file a complaint and appropriate contact information for complaints.

Disputed amendments:

- If the patient wishes to submit a statement of disagreement with the denial, the request must be in writing and should be sent to the Privacy Officer or designee.
- We have the right to require that the statement of disagreement be limited to a reasonable length.
- Upon receipt of the statement of disagreement by the Privacy Officer or designee, he/she may, at his/her discretion, prepare a rebuttal. A copy of the rebuttal must be given to the patient.
- 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.

Disclosure of PHI after request is denied:

- If we disclose 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. We 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, we 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 we receive notification from another provider or covered entity of an amendment to PHI which we have in our possession, the PHI must be amended as applicable and the patient notified according to the criteria in this policy.

- We will retain the documentation of all requests for amendment to records.

Complaints

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

Form(s): **Complaint Log**

Process:

- All complaints related to privacy and patients' PHI should be directed to the Privacy Officer within 24 hours of receipt.
- Complaints that are given verbally should be summarized in writing 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 owner of the practice and the practice's legal counsel.
- All complaints and their disposition will be documented by the Privacy Officer; see attached **Complaint Log**.
- We will not intimidate, threaten, coerce, discriminate against or otherwise retaliate against any patient filing a complaint.
- We will not take any action against any employee or other individual who files a complaint, participates in an investigation or opposes our policies that he/she believes in good faith to be in violation of HIPAA so long as the employee or individual is acting in a reasonable manner and his/her actions do not constitute an unlawful disclosure of PHI.

Specialized Uses and Disclosures

Research

Policy: We may disclose PHI for research purposes only as specified by the process outlined below. *Internal research activities (e.g., quality improvement) that are not planned to be published are not subject to the requirements of this policy*.

Process:

PHI may be disclosed for research only when one of the following three criteria is met:

1. Patient authorization has been given. Authorization may be combined with other written consents/permissions (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.
2. We have provided written notice of disclosures for research purposes and given the patient an opportunity to object AND we have used reasonable efforts to obtain the patient's written authorization.
3. Patient authorization may be established if we mail an authorization to the patient at least two times with a postage prepaid return envelope and conspicuous notice that the patient's medical records may be released if the patient does not object, and at least 60 days have expired since the second notice was sent.

Limited Data Sets

Policy: We may disclose PHI 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 defined below and we have entered into a data use agreement with the recipient.

Form(s): **Data Use Agreement**

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); and
    - 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 [Name of Practice] and the researcher agree that it is needed for purposes of the research; and
    - 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. See **Data Use Agreement**.
- 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:
    - 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;
    - contain language assuring that the recipient will use appropriate safeguards to prevent uses or disclosures of the information other than as permitted by HIPAA or otherwise required by law;
    - limit who can use or receive the limited data set;
    - require the recipient to agree not to re-identify or contact the individual subject;
    - include a requirement to report any improper use or disclosure of which the recipient becomes aware;
- If we are the recipient of PHI under a data use agreement, all provisions of the agreement must be followed.
- 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. We may rely on the requested disclosure as meeting the minimum necessary requirements unless it has reason to suspect that the disclosure does not.
- Employees must verify the validity of all limited data sets with the Privacy Officer *(or designee)* prior to disclosures. It's also prudent for the Privacy Officer to consult with counsel before the Practice creates a limited data set or enters into a data use agreement.

De-Identification

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

Process:

- To be considered de-identified (and no longer PHI), the information must meet one of the following criteria:
    - A qualified statistical expert 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; or

- 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 we may re-identify the information at a later date, if the following criteria are met:
  - Control of the dummy identifier must remain with our office and must not be disclosed.
  - The dummy identifier cannot be derived from individually identifiable information such as a Social Security number.

Marketing

Policy: PHI may be used or disclosed for marketing purposes only as specified in the process outlined below.

Form(s): **Authorization for Marketing Form**

Process:

- We 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 us and any other entity where we disclose PHI in exchange for direct or indirect payment so that the other 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 we do 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 us.

- In addition, the following are NOT considered "marketing":
    - Face-to-face communications with the patient by our office, its providers and/or workforce

- Promotional gifts of a nominal value given to the patient by us, our 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 us for making the communication is reasonably related to our office's cost of making the communication.

- Authorizations for marketing communications for which we receive financial remuneration must include a statement to that effect.

Fundraising

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

Process:

- "Fundraising" is a communication to an individual by us or our business associates for the purposes of raising funds for our office.
- Certain PHI (described below) may be used by us, or disclosed to one of our business associate, 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, our NPP must include a statement that we 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: We will continue to protect a patient's PHI after the patient's death, in accordance with State law and HIPAA.

Process:

- A patient is entitled to protection of his or her PHI even after the patient's death.
- We 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 may disclose PHI to a coroner or medical examiner without consent of a representative for identification purposes, determining a cause of death, or other duties authorized by state law.

Sale of PHI

Policy: We will not sell PHI except as permitted by State law and HIPAA.

Process:

- We will not sell PHI unless it obtains a HIPAA-compliant authorization from the patients who are the subject of the PHI being sold. The authorization must include a statement that we are receiving remuneration in exchange for the PHI.
- A "sale of PHI" is defined as a disclosure of PHI by us, or a business associate of ours, if applicable, where we or our business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

Student Immunizations

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

Process:

- We 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
  - We obtain written 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.

Business Associates

Business Associate Agreements

Policy: We will not disclose PHI to business associates unless current and valid business associate agreements ("BAA"s) are in place or unless otherwise permitted or required by law.

Form(s): **Sample Business Associate Agreement**

Definitions:

Business Associate: A person who, on behalf of our office, but other than in the capacity of a member of our workforce, 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 our workforce, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for us, where the provision of the service involves the disclosure of PHI from us or from a business associate of ours; OR

A Health Information Organization, E-prescribing Gateway or other person that provides data transmission services with respect to PHI to us and that requires access on a routine basis to such PHI; OR

A person that offers a personal health record to one or more individuals on behalf of our office; 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 us to the health care provider concerning the treatment of an individual.

Process:

- It is the responsibility of our Privacy Officer and/or Security Officer to determine which persons or entities are "business associates" of our office.
- We will execute a valid BAA 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. See **Business Associate Agreement**.
- The Privacy Officer will also confirm that each Business Associate that has shared patient PHI with a subcontractor has put in place a BAA with such subcontractor.
- All BAAs must be reviewed by our Privacy Officer to ensure that they meet the requirements of the Privacy Rule. The Privacy Officer should consult with an attorney, as necessary.
- 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 our business associates of any restrictions on the use or disclosure of PHI that we agree affect the business associate's use of the information.

Business Associate Relationships

Policy: We will be conscious of the activities of its business associates and will take actions when it has the reason to believe that the business associate has violated HIPAA and/or the BAA.

Process:

- If we know of a pattern or activity or practice of a business associate that constitutes a material breach of the BAA and/or HIPAA, we will take steps to correct the problem or, if such steps are unsuccessful, terminate the arrangement.
- If any of our employees become aware of a potential problem, he or she should notify the Privacy Officer. The Privacy Officer should notify any other personnel who may be able to assist with the situation, and should take reasonable steps to correct the problem.
- Our office's 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 BAA with the business associate, we will assess the options for termination or allowing a cure period.

Breach Notification Policies and Procedures

Identifying a Breach of Unsecured PHI

Policy: We will identify all breaches of unsecured PHI in order to notify the appropriate parties.

Form(s): **Breach Assessment Form; Breach Log**

Definitions:

Breach: The acquisition, access, use or disclosure of unsecured PHI that is not permitted by HIPAA 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 our office's workforce, a person acting under the authority of our office or one of our 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 our office to another person authorized to access PHI at our office, or by a person authorized to access PHI at one of our 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 we or one of our 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: PHI that we have not rendered unusable, unreadable, or indecipherable to unauthorized persons by or through the use of a technology or methodology specified by the Secretary of HHS (which includes but is not limited to encryption).

Process:

- The Privacy Officer and/or Security Officer will determine whether there has been an acquisition, access, use or disclosure of unsecured PHI that is not permitted by HIPAA. See **Breach Assessment Form** that can be used to assess a breach.
- Any such acquisition, access, use or disclosure of unsecured PHI that is not permitted by HIPAA will be presumed to be a "breach" requiring notification under these policies, UNLESS we 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; for example;
        - Financial information and social security numbers increases the risk of ID theft and financial fraud;
        - 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;
    - Whether the PHI was actually acquired or viewed; and
        - 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.
        - We may be able to obtain and rely on the assurances of another covered entity that it destroyed the information it received in error.
- We will notify our attorney if we are unsure of (i) whether there has been an acquisition, access, use or disclosure of unsecured PHI that is prohibited by HIPAA, and/or (ii) whether there is a low probability that the PHI has been compromised.

- If we demonstrate that there is a low probability that the PHI has been compromised, we will document our 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 we determine the acquisition, access, use or disclosure of PHI that is prohibited by the Privacy Rule does constitute a breach, we will refer to and follow the procedures for breach notification in the sections titled "Notification to Individuals," "Notification to the Media," and "Notification to the Secretary."
- All breaches and their resolution should be logged. See **Breach Log**.

Notification to Individuals

Policy: We will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of a breach by us or one of our business associates, in accordance with the following procedures.

Form(s): **Breach Notification Letter to Individuals**

Process:

- We 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 we knew about the breach, or would have known about the breach if we had exercised reasonable diligence in implementing effective internal policies for discovering breaches of unsecured PHI.
    - If any employee or agent of ours (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.
- We will contact our attorney if we are unsure of (i) the date of discovery of the breach or (ii) whether an individual at our office who caused the breach is an employee or agent of our office.
- 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 we are 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.

- We will use the **Breach Notification Letter to Individuals** as a guide for drafting the notification.
- We 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, we will send the written notification to the next of kin or personal representative of the individual, if we have 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, we will use a substitute form of notice that we believe will reach the individual.
  - If there are fewer than 10 individuals who cannot be reached by mailed written notice, we 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, we will post the notice conspicuously on the home page of our 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, we 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, we 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, we will notify the media in accordance with the policy titled "Notification to the Media."

Notification to the Media

Policy: We will provide notification to the media if a breach of unsecured PHI involved more than 500 residents of one state, county or city.

Form(s): **Media Notification Form**

Process:

- We 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.
- We 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 Individuals" 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. We will use the **Media Notification Form** form as a guide.
- In addition to the notice to the media, we will provide notification of the breach to each individual in accordance with the policy titled "Notification to Individuals" and notification to the Secretary in accordance with the policy titled "Notification to the Secretary."

Notification to the Secretary

Policy: We will provide notification of all breaches of unsecured PHI to the Secretary of Health and Human Services (the "Secretary") as required by HIPAA.

Process:

- We 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:
  - o Date of the breach;
  - o Date of discovery of the breach;
  - o Approximate number of individuals affected by the breach; o Type of breach;
  - o Location of the breached PHI;
  - o Type of PHI involved in the breach;
  - o Brief description of the breach;
  - o Safeguards in place prior to the breach;
  - o Dates the individual notice was provided;
  - o Whether substitute notice was required;
  - o Whether media notice was required; and
  - o Actions taken in response to the breach.

- Within 60 days of the end of the calendar year in which the breaches were discovered, we shall submit electronically a breach notification form for each breach on the Secretary's website: https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html?language=es
- If a breach affects 500 or more individuals, we will electronically submit a breach notification form at the Secretary's website at the same time that we notify the affected individuals.

Employment and Training Issues

Training of Employees

Policy: All of our employees will receive initial and periodic training of our office's HIPAA and State law privacy and security policies and be retrained when changes are made to existing HIPAA or State law requirements or our office's policies.

Form(s): **HIPAA Training Sign-In Sheet**

Process:

- New employees hired will receive HIPAA training during their orientation (i.e., within 14 days of hire) and all employees will receive HIPAA training periodically (i.e., annually).
- Training updates also must be provided whenever HIPAA or State law and/or our office'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.
- We will keep documentation of all employee training provided for at least the six (6) years required by HIPAA. We should use the attached **HIPAA Training Sign-In Sheet** to evidence that employees received the required training.

Discipline and Mitigation for Violations

Policy: We will appropriately discipline any employee who is in violation of our office's HIPAA policies and procedures.

Process:

- As a healthcare provider, we are entrusted with demographic, financial, and clinical information ("PHI") regarding our patients. PHI must be treated with great respect and care by any individual with access to it. Any member of our workforce who uses or discloses PHI in violation of our office's policies and/or HIPAA or State law is subject to formal disciplinary action, up to and including termination, as set forth in this policy and in our 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 us 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 us in these policies);
    - Accessing or reviewing confidential information of another employee that is also one of our patients, without a permissible purpose (permissible purposes are those that are explicitly authorized by us 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.

- We have developed the following discipline/sanctions policy for workforce members who have violated our HIPAA compliance policies. We reserve the right to accelerate these or impose other sanctions, depending on the nature and severity of the violation:
  - First Violation: The Privacy and/or Security Officer will meet privately with the workforce member to review the Practice's policies, procedures and safeguards and make sure that the workforce member understands his/her obligations.
  - Second Violation: The Privacy and/or Security Officer and the Practice owner will follow the steps noted above as well as notify the workforce member, in writing, that further violation will result in suspension.
  - Third Violation: Suspension without pay for five (5) business days as well as notification to the workforce member, in writing, that another violation will result in termination.
  - Fourth (and Final) Violation: Termination.
- The Privacy and/or Security Officer will maintain documentation of all sanctions applied. Documentation will also be placed in the employee's personnel file.

Employee Medical Records

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

Process:

- PHI of employees that is maintained by use in our 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 us in our 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 our office 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: Our employees will not be prevented from or disciplined for reporting violations of HIPAA or State law.

Process:

- A member of our workforce may disclose PHI for "whistleblower" purposes, without violating HIPAA or our office's policies, if the workforce member:
    - Believes in good faith that we have engaged in conduct that is unlawful or violates professional or clinical standards, or that the care, services, or conditions at our office 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 our office's care, or an appropriate accreditation agency to report failure to meet standards to our office'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.
    - Our 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.

Security Risk Assessments and Audits

Security Awareness and Risk Assessments Policy

Policy: We will conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity and availability of its ePHI and develop strategies to efficiently and effectively mitigate the risks identified in the assessment process.

Form(s): ADA Sample Security Risk Assessment for a Small Dental Practice

---

Process:

- The Security Officer will conduct periodic assessments (i.e., at least once every two years) of the potential risks and vulnerabilities to the confidentiality, integrity and availability of our office's ePHI and update the risk analysis, as necessary, to reflect changes in the operating or regulatory environment. In conducting the risk assessment, the Security Officer might consider using the ADA Sample Security Risk Assessment for a Small Dental Practice

- When assessing risks, the Security Officer may take into account:
    - The size, complexity and capabilities of the Practice;
    - The Practice's technical infrastructure, hardware and software security capabilities;
    - The costs of security measures; and
    - The probability and criticality of potential risks to ePHI.

- All workforce members are expected to fully cooperate with the Security Officer in his/her efforts to conduct risk assessments.

- All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, will be documented and maintained for six (6) years.

Audit/Activity Review

Policy: We will conduct audit trails to regularly track the identification and authentication of those accessing computer systems and software that contain electronic PHI ("ePHI").

Process:

General:

- The Security Officer is responsible for reviewing (or coordinating the review of) logs of access and activity to guard against network vulnerabilities and intrusions, breaches in confidentiality and security of patient ePHI, performance problems and flaws in applications and improper alteration or destruction of ePHI. This review should apply to all information applications, systems, networks, and any computing devices, regardless of ownership [e.g., owned, leased, contracted, and/or stand-alone].

- Vulnerability testing software may be used to probe the network. This may be to identify what is running (e.g., operating system or product versions in place). Any publicly-known vulnerability should be corrected. Re-evaluate whether the system can withstand attacks aimed at circumventing security controls.
    - Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party reviewing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be reviewing their own services – separation of duties).
    - Testing shall be done on a routine basis (e.g., annually).

- The process for review of logs, trails, and reports shall include:
    - Description of the activity as well as rationale for performing review;

- Identification of which workforce members or department/unit will be responsible for review (workforce members should not review logs which pertain to their own system activity unless there is no alternative or an inherent conflict of interest);
- Frequency of the reviewing process;
- Determination of significant events requiring further review and follow-up; and
- Identification of appropriate reporting channels for review of results and required follow-up.

Business Associates:

- We should conduct periodic monitoring of business associate and vendor information system activity to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between our office and the external agency.
- If it is determined that the business associate or vendor has exceeded the scope of access privileges, we should reassess the business relationship..
- If it is determined that a business associate has violated the terms of the HIPAA BAA, we must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

External reviews of information access and activity:

- Information system review information and reports gathered from contracted external review firms, business associates and vendors shall be evaluated and appropriate corrective action steps taken as indicated. Prior to contracting with an external review firm, we shall:
    - Outline the review responsibility, authority, and accountability;
    - Choose a review firm that is independent of other organizational operations;
    - Ensure technical competence of the review firm staff;
    - Require the review firm's adherence to applicable codes of professional ethics;
    - Obtain a signed HIPAA-compliant business associate agreement; and

- Assign organizational responsibility for supervision of the external review firm.

Retention of Review Information:

- Reports summarizing review activities shall be retained for a period of six (6) years.

Forms

List of Designated Record Sets		
Date Created: **Date Effective Until:**		
Name of Record Set	**Record Types**	**Record Location (e.g., on-premises, at a business associate, etc.)**

Certificate of Destruction	
Practice should use this form to evidence destruction of electronic PHI	
Date of Destruction:	**Authorized By:**
Description of Information Destroyed/Disposed of:	
Method of Destruction	
☐	Burning
☐	Overwriting
☐	Pulping
☐	Pulverizing
☐	Reformating
☐	Shredding
☐	Other:
Records destroyed by :	
If on-site, witnessed by:	

Designation of Privacy Officer
Privacy Officer Name:
Privacy Officer's Contact Information:
We have designated _____ to serve as its Privacy Officer, effective on the date below, to fulfill the following responsibilities:
Develop and implement privacy and breach notification policies and procedures ("Privacy Policies"), in compliance with HIPAA and State regulations. Stay current on privacy laws and emerging privacy technologies
Train workforce members on their and our office's duties and responsibilities under such Privacy Policies
Work with the Security Officer to periodically assess privacy and security risks
In the event of a breach of the Privacy Policies, oversee sanctions for workforce members responsible for the breach and work with the owner of our practice and outside counsel, as necessary, to respond to customer complaints and/or inquiries/investigations by the Office of Civil Rights or the state attorney general
Work with outside counsel to develop a form of business associate agreement for use with third parties that may have access to customer protected health information and ensure that such agreements are in place with all such third parties
Create and maintain documentation of our office's compliance with its Privacy Policies. Retain such documentation for six (6) years from the date of their creation or the date when last in effect, whichever is later, so as to be prepared for a government investigation or audit
I agree to fulfill the obligations of the Privacy Officer, as denoted above and as required by HIPAA
Privacy Officer's Signature:
Date:

Designation of Security Officer
Security Official Name:
Security Official Contact Information:
We have designated _____ to serve as its Security Officer, effective on the date below, to fulfill the following responsibilities:
Develop and implement policies and procedures to prevent, detect, contain and correct security violations. Stay current on security laws and emerging security technologies
Conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the Practice's electronic PHI and periodically update this risk assessment when there are material changes to the Practice's operating or regulatory environment
In collaboration with the Practice's hardware and software vendors, implement the information system functionality that generates audit logs and access reports on all information systems that contain ePHI. Review systems activity functions, such as audit logs, access reports, and security incident tracking reports validating the performance of safeguard measures
Train workforce members on the Practice's policies and procedures for safeguarding ePHI and on the consequences for failure to comply. Such training will be conducted for each new workforce member and for every workforce member when there are material changes
Investigate, respond to, remediate and document security incidents. Consult with outside counsel and/or compliance consultants, as necessary. Work with outside counsel to develop a form of business associate agreement for use with third parties that may have access to customer protected health information and ensure that such agreements are in place with all such third parties
Select and oversee the installation of appropriate software to encrypt and decrypt ePHI
Create and maintain documentation of our office's compliance with its Security Policies. Retain such documentation for six (6) years from the date of their creation or the date when last in effect, whichever is later, so as to be prepared for a government investigation or audit
I agree to fulfill the obligations of the Security Officer, as denoted above and as required by HIPAA
Security Official's Signature:
Date:

NOTICE OF PRIVACY PRACTICES
[Practice Name]
[Practice Address]

Effective Date of Notice:
Privacy Officer:
Phone Number:
Email:

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

OUR LEGAL DUTY

Federal and state laws require us to maintain the privacy of your health information. We are also required to provide this notice about our office's privacy practices, our legal duties, and your rights regarding your health information. We are required to follow the practices that are outlined in this notice while it is in effect.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided such changes are permitted by applicable law. We reserve the right to make changes in our privacy practices and the new terms of our notice effective for all health information that we maintain, including health information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and make the new notice available upon request. For more information about our privacy practices or additional copies of this notice, please contact our Privacy Officer.

HOW WE MAY USE AND DISCLOSE HEALTH INFORMATION ABOUT YOU

We may use and disclose health information for different purposes, including treatment, payment, and health care operations.

Treatment
We disclose health information to our employees and others who are involved in providing the care you need. For example, we may use or disclose your health information to another dentist or other health care providers providing treatment that we do not provide. We may also share your health information with a pharmacist in order to provide you with a prescription.

Payment
We may use and disclose your health information to obtain payment for services we provide to you. For example, we may send claims to your dental health plan containing certain health information (unless you request that we restrict such disclosure to your health plan when you have paid out-of-pocket and in full for services rendered).

Health Care Operations
We may use and disclose your health information in connection with our health care operations. Health care operations include, but are not limited to, quality assessment and improvement activities, conducting training programs, and licensing or credentialing activities.

Your Family and Friends
We must disclose your health information to you, as described in the Patient Rights section of this notice. You have the right to request restrictions on disclosure to family members, other relatives, close personal friends, or any other person identified by you.

Persons Involved in Your Care
We may use or disclose health information to notify or assist in the notification of (including identifying or locating) a family member, your personal representative, or another person responsible for your care, of your location, your general condition, or your death. If you are present, then prior to the use or disclosure of your health information, we will provide you with an opportunity to

object to such uses or disclosures. In the event of your incapacity or emergency circumstances, we will disclose health information based on a determination using our professional judgment disclosing only health information that is directly relevant to the person's involvement in your health care.

Marketing Health-Related Services
We may contact you about products or services related to your treatment, case management, or care coordination or to propose other treatments or health-related benefits and services in which you may be interested. We may also encourage you to purchase a product or service when you visit our office. If you are currently an enrollee of a dental plan, we may receive payment for communications to you in relation to our provision, coordination or management of your dental care, including our coordination or management of your health care with a third party, our consultation with other health care providers relating to your care or if we refer you for health care. We will not otherwise use or disclose your health information for marketing purposes without your written authorization. We will disclose whether we receive payments for marketing activity you have authorized.

Change of Ownership
If this dental practice is sold or merged with another practice or organization, your health records will become the property of the new owner. However, you may request that copies of your health information be transferred to another dental practice.

Disaster Relief
We may use or disclose your health information to assist in disaster relief efforts.

Required by Law
We may use or disclose your health information when we are required to do so by law.

Public Health
We may, and are sometimes legally obligated to, disclose your health information to public health agencies for purposes related to preventing or controlling disease, injury or disability; reporting abuse or neglect; reporting domestic violence; reporting to the Food and Drug Administration problems with

products and reactions to medications, and reporting disease or infection exposure. Upon reporting suspected elder or dependent adult abuse or domestic violence, we will promptly inform you or your personal representative unless we believe the notification would place you at risk of harm or would require informing a personal representative we believe is responsible for the abuse or harm.

Abuse or Neglect

We may disclose your health information to appropriate authorities if we reasonably believe that you are a possible victim of abuse, neglect, or domestic violence, or the possible victim of other crimes. We may disclose your health information to the extent necessary to avert a serious threat to your health or safety or the health or safety of others.

National Security

We may disclose to military authorities the health information of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials health information required for lawful intelligence, counterintelligence, and other national security activities. We may disclose to correctional institutions or law enforcement officials having lawful custody of protected health information of inmates or patients under certain circumstances.

Secretary of HHS

We will disclose your health information to the Secretary of the U.S. Department of Health and Human Services when required to investigate or determine compliance with HIPAA.

Worker's Compensation

We may disclose your health information to the extent authorized by and to the extent necessary to comply with laws relating to worker's compensation or other similar programs established by law.

Law Enforcement

We may disclose your health information for law enforcement purposes as permitted by HIPAA, as required by law, or in response to a subpoena or court order.

Judicial and Administrative Proceedings
If you are involved in a lawsuit or a dispute, we may disclose your health information in response to a court or administrative order. We may also disclose health information about you in response to a subpoena, discovery request, or other lawful process instituted by someone else involved in the dispute, but only if efforts have been made, either by the requesting party or us, to tell you about the request or to obtain an order protecting the information requested.

Coroners, Medical Examiners, and Funeral Directors
We may release your health information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also disclose your health information to funeral directors consistent with applicable law to enable them to carry out their duties.

Research
We may disclose your health information to researchers for research purposes. In this situation, written authorization is not required as approved by an Institutional Review Board or privacy board that has reviewed the research proposal and established protocols to ensure the privacy of your information.

Fundraising
We may use or disclose demographic information and dates of treatment in order to contact you for fundraising activities. If you no longer wish to receive these communications, notify us at the contact information provided above and we will stop sending further fundraising information.

Your Authorization
We will obtain your written authorization before using or disclosing your health information for purposes other than those provided in this notice (or as otherwise permitted or required by law). You may revoke an authorization in writing at any time. Upon receipt of the written revocation, we will stop using or disclosing your health information, except to the extent that we have already taken action in reliance on the authorization.

PATIENT RIGHTS

Access

You have the right to look at or get copies of your health information, with limited exceptions. You may request that we provide copies in a format other than photocopies. We will use the format you request unless we cannot practicably do so. You must make a request in writing to obtain access to your health information. You may obtain a form to request access by contacting our office. We will charge you a reasonable cost-based fee for expenses such as copies and staff time. You may also request access by sending us a letter. If you request copies, there may be a charge for time spent. If you request an alternate format, we will charge a cost-based fee for providing your health information in that format. If you prefer, we will prepare a summary or an explanation of your health information for a fee. Contact us for a full explanation of our fee structure.

Disclosure Accounting

You have a right to receive a list of instances in which we disclosed your health information for purposes other than treatment, payment, health care operations, and certain other activities for the last six years. If you request this accounting more than once in a 12-month period, we may charge you a reasonable cost-based fee for responding to these additional requests.

Right to Request a Restriction

You have the right to request that we place additional restrictions on our use or disclosure of your health information. We are not required to agree to these additional restrictions, but if we do, we will abide by our agreement (except in an emergency). In the event you pay out-of-pocket and in full for services rendered, you may request that we not share your health information with your health plan. We must agree to this request.

Alternative Communication

You have the right to request that we communicate with you about your health information by alternative means or to alternative locations. You must make your request in writing. Your request must specify the alternative means or location and provide a satisfactory explanation of how payments will be handled under the alternative means or location you request. We will

accommodate all reasonable requests. However, if we are unable to contact you using the ways or locations you have requests we may contact you using the information we have.

Amendment
You have the right to request that we amend your health information. (Your request must be in writing, and it must explain why the information should be amended). We may deny your request under certain circumstances. If we deny your request, we will provide you with a written explanation of why we denied it and explain your rights.

Breach Notification
In the event your unsecured protected health information is breached, we will notify you as required by law. In some situations, you may be notified by our business associates.

Electronic Notice
You may receive a paper copy of this Notice upon request, even if you have agreed to receive this Notice electronically on our Web site or by electronic mail (email).

QUESTIONS AND COMPLAINTS

If you want more information about our privacy practices or have questions or concerns, please contact our Privacy Officer.

If you are concerned that we may have violated your privacy rights, or you disagree with a decision we made about access to your health information or in response to a request you made to amend or restrict the use or disclosure of your health information or to have us communicate with you by alternative means or at alternative locations, you may send a written complaint to our Privacy Officer or to the U.S. Department of Health and Human Services, Office of Civil Rights. We will not retaliate against you for filing a complaint.

Acknowledgment of Receipt of Notice of Privacy Practices
I acknowledge that I have received a copy of the Notice of Privacy Practices of **Name of Practice** and have been offered the opportunity to review it and ask any further questions about my rights to the maintenance of the security of my Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) and corresponding HITECH Legislation.
I understand that I should ask our dental practice's Privacy Officer if I have any questions about the policies and procedures.
Print Name:
Signature:
Date:
For Office Use Only
We attempted to obtain written acknowledgment of receipt of our Notice of Privacy Practices, however, acknowledgment could not be obtained because:
☐ Individual refused to sign
☐ Communications barriers prohibited obtaining acknowledgment
☐ An emergency situation prevented us from obtaining acknowledgment
☐ Other
Employee's Signature:
Date:

Authorization for Use or Disclosure of Patient Information		
Use this form to obtain and document authorization for use or disclosure of patient information that is not permitted or required by HIPAA		
Patient Information		
Name:		DOB:
Telephone:		Chart #:
Description of Information to be Used or Disclosed:		
Purpose of the Use of Disclosure:		
Person(s) who may receive the Information:		
Expiration Date of this Authorization:		
Acknowledgments:		
I hereby authorize the use and disclosure of the above-described information. I understand that such information may be subject to redisclosure by the recipient and may no longer be protected by HIPAA regulations		
I understand that I may revoke this authorization at any time by sending my request in writing to the Practice's Privacy Officer at _____		
I understand that I may refuse to sign this authorization and that my refusal in no way affects my treatment, payment, enrollment in a health plan, or eligibility for benefits		
Patient's Signature:		**Date:**
If a patient's personal representative is the requestor:		
Name of Representative:		**Relationship to the Patient:**
I certify that I have the legal authority under federal and state laws to make this request on behalf of the patient identified above		
Signature of Representative:		**Date:**
Office Use Only		
☐	Copy of signed authorization provided to the individual	Date: Employee's Initials:

Verification of Identity	
Name of Patient:	
Patient's Date of Birth:	Telephone #:
Requestor's Name:	Requestor's Telephone #:
Requestor's Address:	
Description of Patient Information requested:	
Authority of Requestor to Access the Patient Information:	
I certify that the above information is accurate and complete. Requestor's Signature:	Date:
For Office Use Only	
Employee's Name:	
Employee's Signature	
Date:	
If supplied with documentation, what was provided?	
If not supplied with documentation, why not?	

Request for Access	
Patients should use this form to see or request a copy of their own PHI	
Name:	
DOB:	Telephone #:
Records Requested	
Please describe the records requested and the approximate dates of the records:	
Check all that apply	
☐	I would like to see the requested records
☐	I would like to get a copy of the requested records
☐	If the requested records are in an electronic designated data set, I would like an electronic copy of the records in the following form and format, if readily producible:
☐	I would like an email containing the requested records, at the following email address _____, but I understand that unencrypted email is vulnerable to access by third parties.
☐	I would like a summary of the requested records and I agree in advance to pay a fee in the amount of $_____
☐	I would like an explanation of the records that I saw or got a copy of, and I agree in advance to pay a fee of $_____
☐	I would like a copy of the requested records sent to: Name: Address:

Request for Access (page 2)	
Fees: Please note that our office charges a reasonable, cost-based fee to send patients copies of their patient information, and for postage to mail records to patients if requested. A different fee schedule may apply for copies to be sent to third parties upon patient requests or with patient authorization.	
If the patient is the requestor:	
Patient Signature:	Date:
If a patient's personal representative is the requestor:	
Name of Representative:	
Relationship to the Patient:	
I certify that I have the legal authority under federal and state laws to make this request on behalf of the patient identified above.	
Representative's Signature:	Date:
For Office Use Only	
☐	Request for access denied (attach written denial)
☐	Request for access approved

Request for Restricted Use or Disclosure	
Patients should use this form to request a restriction on the use or disclosure of their PHI.	
Patient's Name:	
Patient's DOB:	Telephone #:
(check one)	
☐	I request that the Practice not give information about the following item(s) and/or service(s) for which Practice has been paid in full, to the health plan indicated below, for purposes of payment or health care operations, unless required by law. Item(s) or Service(s): Health Plan: I understand that the Practice must agree to this restriction if it has received payment in full for the Item(s) or Service(s) **OR**
☐	I request that the Practice not use or disclose the information indicated below in the manner indicated below: Description of Information: Requested restricted use or disclosure: I understand that the Practice is not required to agree to this restriction but if it does agree it can end the restriction by telling me. I also understand that if the Practice agrees to this restriction, it may use and disclose the restricted information in certain cases, such as for emergency treatment or public health disclosure.
Patient Signature:	Date:
Dentist/Administrator Signature:	Date:
For Office Use Only	
☐	Agree
☐	Not Agree

Request for Confidential Communications	
Patients should use this form to request that the Practice communicate with them in a different way or a different place.	
Name:	
DOB:	Telephone #:
Patient Requests	
Please describe the records requested and the approximate dates of the records:	
Check all that apply	
☐	I would like the Practice to communicate with me in the manner described below and/or at the following address: If by email, I understand that unencrypted email is vulnerable to access by third parties.
☐	I specify the following as an alternative method of payment:
If the patient is the requestor:	
Patient Signature:	Date:
If a patient's personal representative is the requestor:	
Name of Representative:	
Relationship to the Patient:	
I certify that I have the legal authority under federal and state laws to make this request on behalf of the patient identified above.	
Representative's Signature:	Date:

Request for Accounting of Disclosures and Response	
Patient Information	
Name:	
Telephone #:	DOB:
Accounting-Request	
Please indicate the dates for which you would like to receive an accounting of disclosures of your PHI.	
Note: Under HIPAA, we are not required to include certain disclosures, such as those for treatment, payment, or healthcare operations.	
Start Date:	End Date:
Patient Signature:	
Date:	
Please contact our Privacy Officer at _____ if you have any questions regarding this request.	

Accounting of Disclosures Checklist	
We MUST account for the following types of disclosures:	
☐	For public health activities (e.g., 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 a 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 the 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

Accounting of Disclosures Checklist (page 2)	
We DO 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 counterintelligence)
☐	To law enforcement officials/correctional institutions with custody of the patient
☐	The disclosure occurred more than six years from the date of the request for an 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.	

Log of Disclosures of Patient Information				
The practice may use this form to log disclosures of patient information, so as to facilitate a response to a patient request for an accounting of disclosures.				
Patient Name	**Date of Disclosure**	**Who Received the Information**	**Description of PHI Disclosed**	**Purpose of Disclosure**

Request for Amendment of Records and Response	
Patients should use this form to request that the Practice change the PHI in the Practice's designated record set.	
Patient Information	
Name:	
Telephone #:	DOB:
Amendment Request	
I would like my records changed as follows:	
The reason for the change is as follows:	
If the patient is the requestor:	
Patient Signature:	Date:
If a patient's personal representative is the requestor:	
Name of Representative:	
Relationship to the Patient:	
I certify that I have the legal authority under federal and state laws to make this request on behalf of the patient identified above.	
Representative's Signature:	Date:
Please contact our Privacy Officer at _____ if you have any questions regarding this request.	

Denial of Request to Amend

Practice should use this form to notify a patient that the Practice has denied the patient's request to amend information in a designated record set.

Name:

Address:

Dear [Name of Patient]:

We have reviewed your request to amend your records and have determined that we cannot approve your request because:

☐	The information or record is not in a designated record set
☐	The information or record is accurate and complete
☐	The patient does not have a right to access the information or record
☐	The Practice did not create the information or record

Please note that you have the right to disagree with this denial by sending a written statement of the disagreement to our Privacy Office at _____.

If you believe that we have violated your privacy rights, or disagree with our response to your request, you may file a complaint with our Privacy Officer or with the U.S. Department of Health and Human Services at the following link: https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf.

Amendment Request Log

The practice may use this form to log the Practice's responses to patient requests to amend information in a designated record set.

Patient Name	Requested Amendment	Approved? (Y/N)	Date Amendment Completed	3rd Parties who Must be Notified of the Amendment

Complaint Log					
The practice may use this form to log complaints about the Practice's HIPAA compliance practices					
Patient Name	**Nature of Complaint**	**Date of Complaint**	**Date of Practice's Response**	**Sanctions (if any)**	**Remedial Actions (e.g., training, process changes, etc.)**

Data Use Agreement

Between

[Insert Name of Holder of Protected Health Information]

And

[Insert Name of Data Set Recipient/Researcher]

This Data Use Agreement is made and entered into on [Insert Date] by and between [insert Holder name], hereafter "Holder" and [insert Recipient name], hereafter "Recipient."

1. This agreement sets forth the terms and conditions pursuant to which Holder will disclose certain protected health information, hereafter "PHI" in the form of a Limited Data Set to the Recipient.
2. Terms used, but not otherwise defined, in this Agreement shall have the meaning given the terms in the HIPAA Regulations at 45 CFR Part 160-164.
3. Permitted Uses and Disclosures:

3.1 Except as otherwise specified herein, Recipient may make all uses and disclosures of the Limited Data Set necessary to conduct the research described herein: [include a brief description of the research and/or HSC protocol number] ("Research Project")

3.2 In addition to the Recipient, the individuals, or classes of individuals, who are permitted to use or receive the Limited Data Set for purposes of the Research Project include: [insert names or classes of persons who may use or receive the limited data set, e.g. the researcher's staff, any collaborators, other clinical sites involved in the research, sponsors if applicable, outside laboratories]. To the extent that the classes of persons are not part of the Recipient's workforce who are directly involved in the Research Project, the Recipient shall enter into a data agreement with the other classes of persons before such release of the Limited Data Sets.

4. Recipient Responsibilities:

4.1 Recipient will not use or disclose the Limited Data Set for any purpose other than permitted by this Agreement pertaining to the Research Project or as required by law;

4.2 Recipient will use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Limited Data Set other than as provided for by this Agreement;

4.3 Recipient will report to the Holder any use or disclosure of the Limited Data Set not provided for by this Agreement of which the Recipient becomes aware within 15 days of becoming aware of such use or disclosure;

4.4 Recipient will ensure that any agent, including a subcontractor, to whom it provides the Limited Data Set, agrees to the same restrictions and conditions that apply through this Agreement to the Recipient with respect to the Limited Data Set;

4.5 Recipient will not identify the information contained in the Limited Data Set; and

4.6 Recipient will not contact the individuals who are the subject of the PHI contained in the Limited Data Set.

5. Term and Termination:

5.1 The terms of this Agreement shall be effective as of [insert effective date], and shall remain in effect until all PHI in the Limited Data Set provided to the Recipient is destroyed or returned to the Holder.

5.2 Upon the Holder's knowledge of a material breach of this Agreement by the Recipient, the Holder shall provide an opportunity for Recipient to cure the breach or end the violation. If efforts to cure the breach or end the violation are not successful within the reasonable time period specified by the Holder, the Holder shall discontinue disclosure of PHI to the Recipient and report the problem to the Secretary of the Department of Health and Human Services or its designee. The Holder shall immediately discontinue disclosure of the Limited Data Set to the Recipient if the Holder determines cure of the breach is not possible.

6. General Provisions:

6.1 Recipient and Holder understand and agree that individuals who are the subject of Protected Health Information are not intended to be third party beneficiaries of this Agreement.

6.2 This Agreement shall not be assigned by Recipient without the prior written consent of the Holder.

6.3 Each party agrees that it will be responsible for its own acts and the results thereof to the extent authorized by law and shall not be responsible for the acts of the other party or the results thereof.

IN WITNESS WHEREOF, the parties hereto execute this agreement as follows:
[Name of Holder of Data]
By:
Title:
Date:
[Name of Recipient of Data]
By:
Title:
Date:

Authorization for Marketing

Practice should use this form to obtain patient authorization for the use or disclosure of the patient's information for appropriate marketing communications.

Dear Patient:

From time to time we may like to inform patients about products or services that may be of interest to them. As noted in our Notice of Privacy Practices, before your personal health information ("PHI") is disclosed in communication about a product or service that encourages the use of that product or service, you must authorize this use of your PHI for marketing purposes. Before any health information that can be used to identify you is used in advertising, websites, brochures, or any other promotional materials you must authorize this use of your PHI.

Acknowledgments:

- I hereby authorize [Name of Practice] ("Practice") to use my name and address and other information about my dental health (including with a business associate) to provide marketing communications to me.
- I understand that the practice may receive financial remuneration for marketing communications.
- I understand that the information disclosed may be subject to redisclosure by the recipient and may no longer be protected by HIPAA regulations.
- I understand that I may revoke this authorization at any time, in writing, by providing notice to the Practice's Privacy Officer.

Patient Signature:
Patient Name:
Date:

Business Associate Agreement

This BUSINESS ASSOCIATE AGREEMENT (the "BAA") is made and entered into as of [Date] by and between [Name of Practice] ("Covered Entity") and Dental Office Compliance of New England, a LLC ("Business Associate", in accordance with the meaning given to those terms at 45 CFR §164.501). In this BAA, Covered Entity and Business Associate are each a "Party" and, collectively, are the "Parties".

BACKGROUND

I. Covered Entity is either a "covered entity" or "business associate" of a covered entity as each are defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the HITECH Act (as defined below) and the related regulations promulgated by HHS (as defined below) (collectively, "HIPAA") and, as such, is required to comply with HIPAA's provisions regarding the confidentiality and privacy of Protected Health Information ("PHI," as defined below);

II. The Parties have entered into or will enter into one or more agreements under which Business Associate provides or will provide certain specified services to Covered Entity (collectively, the "Agreement");

III. In providing services pursuant to the Agreement, Business Associate will have access to PHI;

IV. By providing the services pursuant to the Agreement, Business Associate will become a "business associate" of the Covered Entity as such term is defined under HIPAA;

V. Both Parties are committed to complying with all federal and state laws governing the confidentiality and privacy of health information, including, but not limited to, the Standards for Privacy of Individually Identifiable Health

Information found at 45 CFR Part 160 and Part 164, Subparts A and E (collectively, the "Privacy Rule"); and

VI. Both Parties intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to the terms of this Agreement, HIPAA and other applicable laws.

AGREEMENT

NOW, THEREFORE, in consideration of the mutual covenants and conditions contained herein and the continued provision of PHI by Covered Entity to Business Associate under the Agreement in reliance on this BAA, the Parties agree as follows:

1. Definitions. For purposes of this BAA, the Parties give the following meaning to each of the terms in this Section 1 below. Any capitalized term used in this BAA, but not otherwise defined, has the meaning given to that term in the Privacy Rule or pertinent law.

A. "Affiliate" means a subsidiary or affiliate of Covered Entity that is, or has been, considered a covered entity, as defined by HIPAA.

B. "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI, as defined in 45 CFR §164.402.

C. "Breach Notification Rule" means the portion of HIPAA set forth in Subpart D of 45 CFR Part 164.

D. "Data Aggregation" means, with respect to PHI created or received by Business Associate in its capacity as the "business associate" under HIPAA of Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate in its capacity as a business associate of one or more other "covered entity" under HIPAA, to permit data analyses that relate to the Health Care Operations (defined below) of the respective covered entities. The meaning of "data aggregation" in this BAA shall be consistent with the meaning given to that term in the Privacy Rule.

E. "Designated Record Set" has the meaning given to such term under the Privacy Rule, including 45 CFR §164.501.B.

F. "De-Identify" means to alter the PHI such that the resulting information meets the requirements described in 45 CFR §§164.514(a) and (b).

G. "Electronic PHI" means any PHI maintained in or transmitted by electronic media as defined in 45 CFR §160.103.

H. "Health Care Operations" has the meaning given to that term in 45 CFR §164.501.

I. "HHS" means the U.S. Department of Health and Human Services.

J. "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.

K. "Individual" has the same meaning given to that term i in 45 CFR §§164.501 and 160.130 and includes a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

L. "Privacy Rule" means that portion of HIPAA set forth in 45 CFR Part 160 and Part 164, Subparts A and E. Page 3 of 9

M. "Protected Health Information" or "PHI" has the meaning given to the term "protected health information" in 45 CFR §§164.501 and 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

N. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

O. "Security Rule" means the Security Standards for the Protection of Electronic Health Information provided in 45 CFR Part 160 & Part 164, Subparts A and C.

P. "Unsecured Protected Health Information" or "Unsecured PHI" means any "protected health information" as defined in 45 CFR §§164.501 and 160.103 that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS Secretary in the guidance issued pursuant to the HITECH Act and codified at 42 USC §17932(h).

2. Use and Disclosure of PHI.

A. Except as otherwise provided in this BAA, Business Associate may use or disclose PHI as reasonably necessary to provide the services described in the Agreement to Covered Entity, and to undertake other activities of Business Associate permitted or required of Business Associate by this BAA or as required by law.

B. Except as otherwise limited by this BAA or federal or state law, Covered Entity authorizes Business Associate to use the PHI in its possession for the proper management and administration of Business Associate's business and to carry out its legal responsibilities. Business Associate may disclose PHI for its proper management and administration, provided that (i) the disclosures are required by law; or (ii) Business Associate obtains, in writing, prior to making any disclosure to a third party (a) reasonable assurances from this third party that the PHI will be held confidential as provided under this BAA and used or further disclosed only as required by law or for the purpose for which it was disclosed to this third party and (b) an agreement from this third party to notify Business Associate immediately of any breaches of the confidentiality of the PHI, to the extent it has knowledge of the breach.

C. Business Associate will not use or disclose PHI in a manner other than as provided in this BAA, as permitted under the Privacy Rule, or as required by law. Business Associate will use or disclose PHI, to the extent practicable, as a limited data set or limited to the minimum necessary amount of PHI to carry out the intended purpose of the use or disclosure, in accordance with Section 13405(b) of the HITECH Act (codified at 42 USC §17935(b)) and any of the act's implementing regulations adopted by HHS, for each use or disclosure of PHI.

D. Upon request, Business Associate will make available to Covered Entity any of Covered Entity's PHI that Business Associate or any of its agents or subcontractors have in their possession.

E. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

3. Safeguards Against Misuse of PHI. Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as provided by the Agreement or this BAA and Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate agrees to take reasonable steps, including providing adequate training to its employees to ensure compliance with this BAA and to ensure that the actions or omissions of its employees or agents do not cause Business Associate to breach the terms of this BAA.

4. Reporting Disclosures of PHI and Security Incidents. Business Associate will report to Covered Entity in writing any use or disclosure of PHI not provided for by this BAA of which it becomes aware and Business Associate agrees to report to Covered Entity any Security Incident affecting Electronic PHI of Covered Entity of which it becomes aware. Business Associate agrees to report any such event within five business days of becoming aware of the event.

***5.* Reporting Breaches of Unsecured PHI.** Business Associate will notify Covered Entity in writing promptly upon the discovery of any Breach of Unsecured PHI in

accordance with the requirements set forth in 45 CFR §164.410, but in no case later than 30 calendar days after discovery of a Breach. Business Associate will reimburse Covered Entity for any costs incurred by it in complying with the requirements of Subpart D of 45 CFR §164 that are imposed on Covered Entity as a result of a Breach committed by Business Associate.

6. Mitigation of Disclosures of PHI. Business Associate will take reasonable measures to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of any use or disclosure of PHI by Business Associate or its agents or subcontractors in violation of the requirements of this BAA.

7. Agreements with Agents or Subcontractors. Business Associate will ensure that any of its agents or subcontractors that have access to, or to which Business Associate provides, PHI agree in writing to the restrictions and conditions concerning uses and disclosures of PHI contained in this BAA and agree to implement reasonable and appropriate safeguards to protect any Electronic PHI that it creates, receives, maintains or transmits on behalf of Business Associate or, through the Business Associate, Covered Entity. Business Associate shall notify Covered Entity, or upstream Business Associate, of all subcontracts and agreements relating to the Agreement, where the subcontractor or agent receives PHI as described in section 1.M. of this BAA. Such notification shall occur within 30 (thirty) calendar days of the execution of the subcontract by placement of such notice on the Business Associate's primary website. Business Associate shall ensure that all subcontracts and agreements provide the same level of privacy and security as this BAA.

8. Audit Report. Upon request, Business Associate will provide Covered Entity, or upstream Business Associate, with a copy of its most recent independent HIPAA compliance report (AT-C 315), HITRUST certification or other mutually agreed upon independent standards based third party audit report. Covered entity agrees not to re-disclose Business Associate's audit report.

9. Access to PHI by Individuals.

A. Upon request, Business Associate agrees to furnish Covered Entity with copies of the PHI maintained by Business Associate in a Designated Record Set in the time and manner designated by Covered Entity to enable Covered Entity to respond to an Individual's request for access to PHI under 45 CFR §164.524.

B. In the event any Individual or personal representative requests access to the Individual's PHI directly from Business Associate, Business Associate within ten business days, will forward that request to Covered Entity. Any disclosure of, or decision not to disclose, the PHI requested by an Individual or a personal representative and compliance with the requirements applicable to an Individual's right to obtain access to PHI shall be the sole responsibility of Covered Entity.

10. Amendment of PHI.

A. Upon request and instruction from Covered Entity, Business Associate will amend PHI or a record about an Individual in a Designated Record Set that is maintained by, or otherwise within the possession of, Business Associate as directed by Covered Entity in accordance with procedures established by 45 CFR §164.526. Any request by Covered Entity to amend such information will be completed by Business Associate within 15 business days of Covered Entity's request.

B. In the event that any Individual requests that Business Associate amend such Individual's PHI or record in a Designated Record Set, Business Associate within ten business days will forward this request to Covered Entity. Any amendment of, or decision not to amend, the PHI or record as requested by an Individual and compliance with the requirements applicable to an Individual's right to request an amendment of PHI will be the sole responsibility of Covered Entity.

11. Accounting of Disclosures.

A. Business Associate will document any disclosures of PHI made by it to account for such disclosures as required by 45 CFR §164.528(a). Business

Associate also will make available information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosures in accordance with 45 CFR §164.528. At a minimum, Business Associate will furnish Covered Entity the following with respect to any covered disclosures by Business Associate: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI, and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure which includes the basis for such disclosure.

B. Business Associate will furnish to Covered Entity information collected in accordance with this Section 10, within ten business days after written request by Covered Entity, to permit Covered Entity to make an accounting of disclosures as required by 45 CFR §164.528, or in the event that Covered Entity elects to provide an Individual with a list of its business associates, Business Associate will provide an accounting of its disclosures of PHI upon request of the Individual, if and to the extent that such accounting is required under the HITECH Act or under HHS regulations adopted in connection with the HITECH Act.

C. In the event an Individual delivers the initial request for an accounting directly to Business Associate, Business Associate will within ten business days forward such request to Covered Entity.

12. Availability of Books and Records. Business Associate will make available its internal practices, books, agreements, records, and policies and procedures relating to the use and disclosure of PHI, upon request, to the Secretary of HHS for purposes of determining Covered Entity's and Business Associate's compliance with HIPAA, and this BAA.

13. Responsibilities of Covered Entity. With regard to the use and/or disclosure of Protected Health Information by Business Associate, Covered Entity agrees to:

A. Notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

B. Notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

C. Notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

D. Except for data aggregation or management and administrative activities of Business Associate, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

14. Data Ownership. Business Associate's data stewardship does not confer data ownership rights on Business Associate with respect to any data shared with it under the Agreement, including any and all forms thereof. 15. Term and Termination.

A. This BAA will become effective on the date first written above, and will continue in effect until all obligations of the Parties have been met under the Agreement and under this BAA.

B. Covered Entity may terminate immediately this BAA, the Agreement, and any other related agreements if Covered Entity makes a determination that Business Associate has breached a material term of this BAA and Business Associate has failed to cure that material breach, to Covered Entity's reasonable satisfaction, within 30 days after written notice from Covered Entity. Covered Entity may report the problem to the Secretary of HHS if termination is not feasible.

C. If Business Associate determines that Covered Entity has breached a material term of this BAA, then Business Associate will provide Covered Entity with written notice of the existence of the breach and shall provide Covered

Entity with 30 days to cure the breach. Covered Entity's failure to cure the breach within the 30-day period will be grounds for immediate termination of the Agreement and this BAA by Business Associate. Business Associate may report the breach to HHS.

D. Upon termination of the Agreement or this BAA for any reason, all PHI maintained by Business Associate will be returned to Covered Entity or destroyed by Business Associate. Business Associate will not retain any copies of such information. This provision will apply to PHI in the possession of Business Associate's agents and subcontractors. If return or destruction of the PHI is not feasible, in Business Associate's reasonable judgment, Business Associate will furnish Covered Entity with notification, in writing, of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of the PHI is infeasible, Business Associate will extend the protections of this BAA to such information for as long as Business Associate retains such information and will limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible. The Parties understand that this Section 14.D. will survive any termination of this BAA.

15. Effect of BAA.

A. This BAA is a part of and subject to the terms of the Agreement, except that to the extent any terms of this BAA conflict with any term of the Agreement, the terms of this BAA will govern.

B. Except as expressly stated in this BAA or as provided by law, this BAA will not create any rights in favor of any third party.

16. Regulatory References. A reference in this BAA to a section in HIPAA means the section as in effect or as amended at the time.

17. Notices. All notices, requests and demands or other communications to be given under this BAA to a Party will be made via either first class mail, registered or certified or express courier, or electronic mail to the Party's address given below:

A. If to Covered Entity, to: [name and address]

B. If to Business Associate, to: [name and address]

18. Amendments and Waiver. This BAA may not be modified, nor will any provision be waived or amended, except in writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

19. HITECH Act Compliance. The Parties acknowledge that the HITECH Act includes significant changes to the Privacy Rule and the Security Rule. The privacy subtitle of the HITECH Act sets forth provisions that significantly change the requirements for business associates and the agreements between business associates and covered entities under HIPAA and these changes may be further clarified in forthcoming regulations and guidance. Each Party agrees to comply with the applicable provisions of the HITECH Act and any HHS regulations issued with respect to the HITECH Act. The Parties also agree to negotiate in good faith to modify this BAA as reasonably necessary to comply with the HITECH Act and its regulations as they become effective but, in the event that the Parties are unable to reach agreement on such a modification, either Party will have the right to terminate this BAA upon 30- days' prior written notice to the other Party.

In light of the mutual agreement and understanding described above, the Parties execute this BAA as of the date first written above.

[ ]("Covered Entity")

By: _____

Name: _____

Title: _____

[ ]("Business Associate")

By: _____

Name: _____

Title: _____

Breach Assessment
Practice should use this form to assess a suspected breach of unsecured PHI.
Basic Facts:
What Information was disclosed:
To whom the information was disclosed (e.g., a business associate(s), other patients, etc.) and whether such recipients actually reviewed the information:
From where (e.g., laptop, desktop computer, server, email, other portable device, electronic file, paper, etc.) and how the information was disclosed (i.e., theft, loss, improper disposals, unauthorized access, hacking, other):
Frequency and duration of the disclosure (i.e., one time or more than once, for a period of time?):
Assessment under HIPAA
Was the disclosure impermissible under HIPAA?
Remedial actions that are taken or to be taken (e.g., process improvements, notifications, sanctions, etc.):
This assessment is accurate and complete.
Name of Privacy Officer:
SIgnature of Privacy Officer:
Date of Assessment:

Breach Log
Date of the breach:
Date of the discovery of the breach:
The approximate number of individuals affected by the breach:
Type of breach (e.g., unauthorized disclosure, hacking, etc.):
Location of the breached PHI (e.g., laptop, other portable device, paper files, etc.):
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:
Was a substitute notice was required?
Was a media notice was required?
Actions taken in response to the breach:

Sample Breach Notification Letter to Individuals

Practice should use this letter to notify impacted individuals about a breach of their PHI.

[PRACTICE LETTERHEAD]

[Date]
[Patient Name/Address]

Dear [Patient]:

We regret to inform you that our practice has discovered a [potential] breach of your personal health information. We became aware of this breach on [date]. We believe that information containing your [describe the types of unsecured protected health information involved: name, address, social security number, date of birth, diagnosis, other] was (briefly describe what happened: stolen, inadvertently disclosed to a third party, other) on [date].

We advise you to immediately take the following steps:

- Call the toll-free numbers of any of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three bureaus will provide you a copy of your credit report free of charge.

  Equifax: (888)766-0008; www.fraudalerts.equifax.com. General: (800) 685-1111, www.equifax.com, P.O. Box 740241, Atlanta, GA 30374-0241.

  Experian: (888) 397-3742; https://www.experian.com/fraud/center.html. General: (888)EXPERIAN (397-3742); www.experian.com; 475 Anton Blvd., Costa Mesa, CA 92626.

  TransUnion: (800) 680-7289 (888-909-8872 for freeze); http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page; TransUnion Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA

19022-2000. General: (800) 680-7289; www.transunion.com; P.O. Box 2000, Chester, PA 19022-2000

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information. [Option – one way to mitigate harm: To help ensure that this information is not used inappropriately, we will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, [describe what the patient needs to do to obtain this service.]

We are investigating how this breach happened by [describe what you are doing to investigate the breach].

We are committed to lessening the harm this may cause you by [describe your mitigation efforts/plans].

To protect against such breaches in the future, we [describe how you will protect against further breaches: recently upgraded our security standards and have purchased encryption software, changed shredding companies, changed the locks on our doors, password protected all of our computers, other].

We apologize for the stress and worry this situation has caused you. We are committed to keeping your information safe and assure you we are doing everything possible to regain your trust in our practice.

Please do not hesitate to contact us with any questions about this incident or if you need additional information on what you should do as a result of the breach, at [toll-free telephone number, email address, website, and/or mailing address].

Sincerely,

[Dentist's Name]

[Dentist's Signature]

Sample Media Notification

Practice should use this letter to notify the media about a breach of patient PHI.

[Date]

Contact: [Name and contact information for Privacy Officer]

IMMEDIATE PRESS RELEASE

PATIENTS NOTIFIED OF BREACH OF UNSECURED PERSONAL INFORMATION

[Name of Practice] notified [Insert Number] patients of a breach of unsecured personal patient protected health information (PHI) after discovering the following event:

[Insert the information from the letter that was sent to the patients]

In conjunction with [law enforcement and security experts, if applicable], [Name of Practice] is working to notify impacted patients to mitigate the damages of the breach. [Name of Practice] has in place safeguards to ensure the privacy and security of all patient health information. As a result of this breach, steps are underway to further improve the security of its operations and eliminate future risks.

In a notification to patients, [Name of Practice] has offered their resources as well as [Insert as Applicable]. [Name of Practice] also has encouraged its patients to contact their financial institutions to prevent unauthorized access to personal accounts. [Name of Practice] has trained staff available for patients to call with any questions related to the data breach. Patients may call [Insert Phone Number Here] from 8:00 am to 4:30 pm Monday through Friday with any questions or concerns. [In addition, patients may visit [Name of Practice]'s Website at www._____ for further information.]

"We understand the importance of safeguarding our patients' personal information and take that responsibility very seriously," said [Insert dentist's name], the president and owner of [Name of Practice]. "We will do all we can to work with our patients whose personal information may have been compromised and help them work through the process. We regret that this incident has occurred, and we are committed to preventing such future occurrences."

HIPAA Training Sign-In Sheet		
Date:		**Duration of Training:**
Instructor:		
Instructor's Qualifications:		
Topic(s) Covered:		
Attendance		
Name	**Job Title**	**Signature**