AMERICAN ASSOCIATION OF ORTHODONTISTS

GUIDE TO PATIENT PRIVACY AND SECURITY RULES

I. INTRODUCTION

The American Association of Orthodontists ("AAO") has prepared this *Guide* and the attachment to assist its members in understanding the privacy and security rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information for Economic and Clinical Health Act ("HITECH"), which was enacted as a part of the American Reinvestment and Recovery Act of 2009. The purpose of this *Guide* is to provide AAO members with the general background and the key concepts and terms of the rules so that they can assess their policies and procedures as to patient privacy and security. However, because each practice is different and there may be unique state laws that apply to a specific case, members should consult with their legal counsel prior to implementing any material in this publication.

II. GENERAL BACKGROUND

In 1996, the U.S. Congress passed the Administrative Simplification provisions of HIPAA to give people greater control over the privacy of their medical information, to help them transfer health insurance between employers, and to lower the costs involved in transmitting this information. In 2009, HITECH was enacted to modify certain provisions of HIPAA and to strengthen its privacy and security provisions. HITECH also added a new rule on breach notification.

There are federal regulations implementing both HIPAA and HITECH (the "HIPAA Regulations"). There are four main components to the HIPAA Regulations – the HIPAA Privacy Rule, the HIPAA Security Rule, the HIPAA Breach Notification Rule and the HIPAA Enforcement Rule.

On January 25, 2013, the long-awaited HIPAA Final Omnibus Rule (the "Final Rule") was published. The Final Rule implemented changes to HIPAA, and the HIPAA Regulations – including the final modifications mandated by HITECH. Some of the more notable changes implemented by the Final Rule are discussed below.

III. OVERVIEW OF KEY CONCEPTS AND TERMS

A. Covered Entities

HIPAA and the HIPAA Regulations generally apply to health plans, health care clearinghouses, and to any health care provider (including an orthodontist) who transmits "protected health information" (also referred to as "PHI," as described below) in electronic form in connection with certain covered transactions for which the Secretary of the U.S. Department of Health and Human Services ("HHS") has adopted standards under HIPAA (*i.e.*, a request to obtain payment,

and necessary accompanying information, from a health care provider to a health plan). Each of these entities is considered a "covered entity" under HIPAA.

Note: HIPAA and the HIPAA Regulations do not apply to AAO members who transmit health information only in paper form or via facsimile. However, if patient information is transmitted electronically in connection with a standard transaction, *all* PHI of that orthodontist is covered, regardless of whether it is in electronic form.

B. Business Associates

HIPAA also applies (under HITECH) to persons or entities that perform or assist in the performance of certain activities for or on behalf of a covered entity, if the performance of the services involves the use or disclosure of PHI (*e.g.*, attorneys, accountants, billing companies, etc.). Such an entity is referred to as a "business associate" under HIPAA. The Final Rule made some clarifications and additions to the types of entities that meet the HIPAA definition of a business associate. For instance, health information organizations, e-prescription gateways, data transmission services that require routine access to PHI, and entities that maintain PHI but do not actually view the PHI or only do so on a random or infrequent basis (such as storage companies or cloud-computing companies) are now explicitly included in the HIPAA definition of a business associate.

C. Business Associate Agreements

When a covered entity uses a contractor or other non-workforce member to perform "business associate" activities and services, HIPAA requires that the covered entity and the business associate enter into a "Business Associate Agreement" (also referred to as a "BAA") In a BAA, a covered entity must, among other things, impose specified written safeguards on the PHI used or disclosed by its business associate and require the business associate to report any use or disclosure of such information not authorized by the agreement.

The Final Rule also requires additional elements be included in a BAA, such as (i) a statement that the business associate must comply with Subpart C, of Part 164 of the HIPAA Security Rule; (ii) a statement that the business associate must report breaches of unsecured PHI to the covered entity; (iii) a statement that the business associate must obtain satisfactory assurances (in the form of a written BAA) from any subcontractor that creates or receives PHI on behalf of the business associate that the subcontractor agrees to the same restrictions and conditions that apply to the business associate with respect to such information; and (iv) to the extent the business associate is delegated to carry out a covered entity's obligations under the HIPAA Privacy Rule (*e.g.*, responding to accounting of disclosures or providing an individual with a notice of privacy practices or access to PHI), the business associate must comply with the requirements of the HIPAA Privacy Rule that apply to the covered entity in the performance of such delegated obligations.

D. Protected Health Information

HIPAA protects all "individually identifiable health information" held or transmitted by a covered entity or a business associate, in any form or media, whether electronic, paper, or oral. HIPAA calls this information "protected health information" (or "PHI").[1] "Individually identifiable health information" is information, including demographic data, that relates to: (a) the individual's past, present or future physical or mental health or condition; (b) the provision of health care to the individual; or (c) the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers and demographics (*i.e.*, name, address, birth date, Social Security Number) and all kinds of medical data such as diagnoses, prescriptions, medication history, bills, and patient education materials. Note: Demographic information does not have to be linked to medical data in order to be considered PHI. If individually identifiable health information is "de-identified"[2] and provides no reasonable basis to identify an individual, then there are no restrictions on the use or disclosure of such de-identified health information.

E. The Privacy Rule Requirements

The Privacy Rule, as amended by HITECH, generally establishes requirements to protect PHI maintained and used by a covered entity or a business associate. Among numerous other requirements, the HIPAA Privacy Rule: (i) limits certain uses and disclosures of PHI; (ii) limits most disclosures of PHI to the minimum necessary for the intended purpose; (iii) requires patient authorizations for certain uses and disclosures of PHI; (iv) guarantees patients the right to access their medical records and to know who else has accessed them; (v) establishes requirements for breach notification; and (vi) imposes criminal and civil sanctions for improper uses or disclosures of PHI. The HIPAA Privacy Rule requires a covered entity and, to a certain extent, a business associate to have policies in place addressing these requirements and to maintain those policies for 6 years from the date of creation. **Attachment 1** is a sample of a basic set of privacy policies and procedures. Again, members should consult with their legal counsel prior to implementing such policies and procedures.

Under the Privacy Rule, the basic concept is that a covered entity may use and disclose a patient's PHI only (i) as the patient permits (*e.g.*, through an authorization); or (ii) as permitted under the HIPAA Regulations.

---

[1] Employment records are excluded from the definition of PHI unless used in connection with the provision of treatment of the employee in the employee's role as a patient of the orthodontist.

[2] There are two ways to de-identify information: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required (as indicated at 45 C.F.R. §164.502(d)), and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual. On November 26, 2012, HHS' Office for Civil Rights published formal guidance regarding methods for de-identification of PHI in accordance with HIPAA.

A covered entity health care provider (like an orthodontist) is permitted to use and disclose PHI for, among other things: (1) treatment; (2) payment; and (3) health care operations. These core health care activities are defined in the Privacy Rule:

- **Treatment** is generally defined as the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultations about the patient with other orthodontists, oral surgeons, periodontists, general dentists, etc. and the referral of a patient by one provider to another.

- **Payment** encompasses activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual (*i.e.*, determinations of coverage eligibility, billing, collection activities, and utilization review).

- **Health care operations** include the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) the sale or purchase of a practice (and the due diligence process relating thereto); and (e) business management and general administrative activities of the entity.

There are a number of other uses and disclosures permitted under the Privacy Rule, such as a use or disclosure required by law, for public health activities, to the Food and Drug Administration (in certain circumstances), to law enforcement or for law enforcement purposes, to a health oversight agency, in judicial and administrative proceedings, to avert a serious threat or health or safety, for research, to the military and correctional institutions and to the extent necessary to comply with worker's compensation laws. These permitted uses and disclosures are described in more detail in **Attachment 1**. A use or disclosure of PHI for any purpose other than treatment, payment and health care operations should be carefully evaluated to determine if it fits into an exception under the Privacy Rule.

Moreover, a covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request (known as the "Minimum Necessary Rule"). When the Minimum Necessary Rule applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. The Minimum Necessary Rule is not imposed in all circumstances; for example, it is not imposed on a disclosure to or a request by a health care provider for treatment or a use or a disclosure that is required by law.[3]

[3] The Privacy Rule does not require that every risk of an incidental use or disclosure of PHI be eliminated A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise

If a use or disclosure is not permitted under the HIPAA Regulations, a written authorization must be obtained from the patient. For example, a written authorization must be obtained to use or disclose PHI for marketing purposes (regardless of whether remuneration is received). Marketing does not include face-to-face communications to the patient as to treatment options, providing gifts of nominal value, or communications to describe health-related products or services that are provided by the orthodontist.[4]

The orthodontist generally may *not* condition treatment on the patient signing an authorization (unless, for example, the patient's PHI will be used for research). The patient may revoke the authorization at any time in writing, except to the extent that it has been relied on by the orthodontist. The authorization form must be obtained prior to the disclosure of any PHI for which an authorization is required. The Privacy Rule contains certain requirements for authorizations, including: (i) a description of the PHI to be used or disclosed; (ii) identification of who is authorized to make the requested use or disclosure; (iii) identification of to whom the authorized use or disclosure will be made; (iv) a statement of the purpose of the use or disclosure; (v) the date or event upon which the authorization will expire; (vi) an indication that the patient has the right to revoke the authorization in writing, unless it has been relied upon prior to the time of revocation; (vii) statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient(s) and no longer protected by the Privacy Rule; and (viii) a statement that treatment will not be conditioned on signing the authorization, except where allowed by law (e.g., for research). The authorization must be dated and signed by the patient. It should be retained for at least six (6) years after signature by the patient.

Under the Privacy Rule, covered entities are also required to (i) appoint a "privacy officer" to be responsible for the development and implementation of the privacy policies and procedures; (ii) designate a contact person to be responsible for receiving complaints and responding to inquiries about privacy matters (often times this is the privacy officer); (iii) provide privacy training to all staff members who have access to PHI (this training should be documented).[5]

F. The Security Rule Requirements

The Security Rule, as amended by HITECH, generally requires a covered entity and a business associate to implement administrative, physical, and technical safeguards to ensure the privacy and confidentiality of PHI when it is electronically stored, maintained, or transmitted. Under the Security Rule, certain specifications of safeguards are required and other specifications of

---

permitted use or disclosure is permitted as long as the orthodontist has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the minimum necessary.

[4] Under the Final Rule, if a health care provider receives financial remuneration from a third party in exchange for using PHI to make a communication about a health-related product or service, the communication is considered "marketing" and the provider must obtain a patient's authorization prior to actually making the communication. Further, the authorization must include an acknowledgment that the provider is receiving financial remuneration from a third party for making the communication.

[5] Each new staff member should be trained within a reasonable time after commencement of employment.

safeguards are suggested or "addressable." In determining whether to implement an "addressable" specification, a covered entity must assess whether the specification is a reasonable and appropriate safeguard in its environment, taking into consideration the specification's contribution to protecting the covered entity's electronic PHI, the size, complexity, and capabilities of the covered entity, the covered entity's technical infrastructure, hardware, and software security capabilities, the cost of the security measure, and the probability and criticality of potential risks to the electronic PHI. Following such an assessment, the covered entity must implement the specification if it is reasonable and appropriate; or, if not, document why it would not be reasonable and appropriate, and implement an alternative measure. The safeguards required by the Security Rule and their corresponding implementation specifications are usually set forth in policies and procedures.

HHS recognizes that all risk of disclosure cannot be eliminated and overheard conversations are unavoidable. Thus, restructuring or soundproofing a facility, or retrofitting for private rooms, is not required. Likewise, patient sign-in sheets in an orthodontist's waiting room and conferring with others in the treatment bay area do not violate the rule. However, ensuring the information disclosed is appropriately limited on sign-up sheets, adding curtains, dividers, shields, screens or similar barriers to areas where oral communications often occur between orthodontists and their patients may be required as a "reasonable effort" to provide privacy safeguards. Likewise, lowering voices and asking waiting patients to stand a few feet away from a counter used for patient counseling or scheduling appointments would be considered a "reasonable effort."

The Security Rule also requires a covered entity and a business associate: (i) to have policies and procedures in place addressing the safeguards; (iii) to maintain those policies for six (6) years from the date of creation; and (iii) to appoint a "privacy officer" who is responsible for the development and implementation of the policies and procedures required by the Security Rule.

G. Patient Rights

The HIPAA Regulations provide patients with a number of rights with respect to their PHI. Those rights include:

1. A right to receive a written notice as to how their PHI will be used and disclosed and how they can gain access to the information.

This notice is referred to as a Notice of Privacy Practices ("NPP"). It should be provided to the patient at the first office visit, unless the patient presents an emergency situation, in which case it should be obtained as soon as practicable. The Privacy Rule requires the NPP to include, among other things : (i) a description of the uses and disclosures of PHI that may be made for treatment, payment and health care operations; (ii) a description of each of the purposes for which the law allows the orthodontist to use or disclose the patient's PHI without obtaining the individual's authorization; (iii) a statement that other uses will be made only with the patient's authorization, and that such authorization may be revoked; (iv) a description of the patient's rights with respect to their PHI (e.g., that a patient has a right to receive notice if there is a breach of his/her unsecured PHI and the patient has the right to request a restriction on the disclosure of information to a health plan if the information relates solely to an item or service for which the patient has paid out of pocket in full (discussed below); (v) if the health care provider intends to

contact the patient to raise funds, the patient will have the opportunity to opt-out of receiving such communications[6]; (vi) the name, title and telephone number of the orthodontist's contact person where the patient may obtain further information about the orthodontist's privacy practices or submit a complaint).

The NPP should be signed by the patients to indicate that they have received a copy of it. If the patient refuses to sign the notice, the refusal must be documented. The signed notice should be retained for six (6) years. If there is a material change to the notice, the revised notice must be made available to an individual upon the individual's request. A health care provider is also required to have the revised NPP available and posted in a clear and prominent location at the care delivery site (*i.e.*, orthodontist's office).

2. A right to inspect and obtain copies of their PHI.

The orthodontist has 30 days after receiving a request for access or copies from a patient in which to provide the access or information. 60 days is allowed for a response if the records are maintained off-site. A 30-day extension may be obtained if, within the initial 30-day period, the orthodontist provides written notice to the patient of the reasons for the delay and gives a date on which a response will be given. Requests for access or copies from a patient should be in writing.

Under the Final Rule, a health care provider is required to give a patient, upon the patient's request, an electronic copy of PHI that is maintained electronically in a designated record set. For health care providers (like orthodontists), this means that if a provider maintains its medical records electronically, the provider must be able to provide a patient with his/her records on a disc or via secure email formatted as a PDF or Word file, or through a secure web-based portal within 30 days of the patient's request (or within 60 days if the provider gives the patient proper notice of its need for an extension). A provider can charge the patient a "reasonable, cost-based fee" to provide the electronic copy of the PHI. This fee may include (i) technical staff time spent creating and copying the electronic file, such as compiling, extracting, scanning and burning PHI to media; (ii) the cost of supplies for creating electronic media (e.g., discs, flash drives, etc.); and (iii) the cost of postage if the patient requests that the portable media be sent by mail or courier.[7]

---

[6] Under the Final Rule, a health care provider can use a patient's PHI for purposes of making a communication about raising funds for the provider; however, the patient receiving the fund-raising communication (in writing or over the phone) must be provided with a clear and conspicuous opportunity to opt-out of receiving any further fundraising communications. If the patient opts-out of receiving future fundraising communications, the provider must treat the patient's choice to opt-out as a revocation of the patient's authorization to use his or her PHI for fundraising communications.

[7] Note, however, charging a patient a "handling" fee for a copy of his or her records is still not permitted and health care providers must still comply with relevant state law requirements related to charging patients for copies of their medical records – regardless of whether the copy is provided in paper or electronic form. Providers should consider how they will handle these requests, implement appropriate policies and procedures, and train workforce members on this new requirement.

3. A right to amend or modify their PHI.

Although there are exceptions set out in the rule, patients generally have the right to ask their orthodontist to amend their PHI. Such a request should be made in writing. If the practitioner amends the information, a list of persons or entities that the individual wants the covered entity to inform of the amendment must be obtained from the patient, along with an authorization to inform them. The orthodontist must then undertake reasonable efforts to notify those persons and entities of the amendment. However, orthodontists are allowed to deny the patient's request if, among other reasons, the information is accurate and complete, or the orthodontist did not create the information. If the practitioner denies the request, it must be denied in writing. Any written denial must also advise the patient of the reasons for the denial, allow the patient to submit a "written disagreement," state that the individual may ask that the request to amend and the denial be included with any future disclosure of the subject information (if no "written disagreement" is submitted), and mention the patient's right to file a complaint with the Secretary of HHS.

4. A right to request restrictions on the use and disclosure of their PHI

Although patients are allowed to request restrictions on the use and disclosure of their PHI, orthodontists are not obligated to honor the request – except as provided below. If the orthodontist agrees to the request, he/she must adhere to it unless the patient presents an emergency situation.

Under the Final Rule, if a patient asks a health care provider to restrict the disclosures of his/her PHI to a health plan made for payment and health care operations purposes and the PHI pertains solely to a health care item or service for which the patient (or someone acting on the patient's behalf) has paid the provider in full, the health care provider must agree to the restriction. While a provider is not required to create a separate medical record or otherwise segregate PHI subject to such a restriction, a provider will need to flag or use some other method to identify portions of the record that contain PHI subject to the restriction in order to ensure it is not inadvertently sent or made accessible to the health plan for payment or health care operations purposes (*e.g.*, during audits by the health plan).

5. A right to request confidential communication of their PHI.

A patient may, for example, request that the communication of his or her PHI be made by alternative means (*i.e.,* sending correspondence to the patient's office rather than to his or her home). If such a request is made, the orthodontist must comply with it if the request is reasonable. The orthodontist may not inquire as to the reasons for the request. However, the patient can be asked to provide this request in writing, which is generally advisable.

6. A right to receive an accounting of certain disclosures made by their orthodontist of their PHI.

Patients have the right to receive an accounting of certain disclosures of their PHI made by their orthodontist within 6 years from the date of the request. The accounting must include: the date of disclosure; the name and address of the person or entity who received the PHI; a brief description of the information disclosed; and, a brief description of the purpose for the

disclosure. There are several exceptions to this requirement, e.g., disclosures relating to treatment, payment, or health care operations, disclosures made pursuant to an authorization that has been signed by the patient; and incidental disclosures. Any request for an accounting must be responded to within 60 days of the request. An additional 30 days can be obtained if, within the initial 60-day period, the orthodontist notifies the patient in writing of the reasons for the delay and provides a date on which a response will be given. A patient is entitled to one free accounting within a 12-month period. Orthodontists are permitted to charge a reasonable fee for each additional accounting if the orthodontist gives the patient notice of the fee at the time of the request.

7. A right to be notified if there is a breach of their unsecured protected health information.

As described in more detail below, a patient has the right to be notified within 60 days following the discovery of a breach of his/her unsecured PHI.

H. Breach Notification Rule

Under the Breach Notification Rule (which implements a section of HITECH), covered entities and their business associates are required to provide notification following a breach of unsecured[8] protected health information. A "breach" is defined as the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of such information. There are 3 exceptions to this definition:

(i) Any unintentional acquisition, access or use of PHI by a workforce member or individual acting under the authority of a covered entity or a business associate if such access or use was made in good faith and within the scope of authority and does not result in a further unauthorized use or disclosure;

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, and the information is not further used or disclosed in an impermissible manner; and

(iii) A disclosure of PHI where a covered entity or business associate 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.

Under the Final Rule, any unauthorized use or disclosure of PHI that does not meet one of the "breach" exceptions is presumed to be a "breach" unless the provider can demonstrate (through a written risk assessment) that there is a "low probability that the PHI has been compromised." The 4 factors that must be considered include:

[8] Unsecured protected health information is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance.

1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2) the unauthorized person who used the PHI or to whom the disclosure was made;

3) whether the PHI was actually acquired or viewed; and

4) the extent to which the risk to the PHI has been mitigated.

A provider may consider other factors (as appropriate), but the risk assessment must be documented, thorough, completed in good faith and the conclusions reached must be reasonable. However, a provider has the discretion to provide the required notifications following an impermissible use or disclosure of PHI without performing a risk assessment.

Because the Final Rule creates the presumption that a breach has occurred following every impermissible use or disclosure of PHI, providers may decide to make required breach notifications without evaluating the probability that the PHI has been compromised. Ultimately, a provider has the burden to prove that all notifications were provided or that an impermissible use or disclosure did not constitute a breach (by demonstrating through a risk assessment that there was a "low probability that the PHI had been compromised"). Covered entities and business associates must maintain documentation sufficient to meet that burden of proof.

Following a breach of unsecured PHI, providers must provide notification of the breach to affected individuals, the Secretary of HHS, and, in certain circumstances, to the media – as set forth below. In addition, business associates must notify covered entities that a breach has occurred.

- **Notice to the Individual(s)**

Providers must notify affected individuals following the discovery of a breach of unsecured PHI. Providers must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the provider has insufficient or out-of-date contact information for 10 or more individuals, the provider must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the provider has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

- **Notice to the Media**

Providers that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Providers will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- **Notice to the Secretary**

In addition to notifying affected individuals and the media (where appropriate), providers must notify the Secretary of breaches of unsecured PHI. Providers will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

- **Notification by a Business Associate**

If a breach of unsecured PHI occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

I. Enforcement

Under the HIPAA Enforcement Rule, HHS' Office for Civil Rights ("OCR") and state Attorneys General may impose sanctions on covered entities and business associates for the failure to comply with requirements of the HIPAA, including civil penalties ranging from $100 to $50,000 per HIPAA violation. Under HITECH, the maximum penalties that can be applied for additional violations in any one year are within a range of $25,000 to $1,500,000. HHS is required to impose a civil monetary penalty (CMP) if a violation is found to constitute willful neglect of the law. The Final Rule implemented the following tiered penalties to reflect the level of the entity's culpability:

Violation Category	Each Violation	All Such Violations of an Identical provision in Calendar Year
Did Not Know	$100-$50,000	$1.5 million

Reasonable Cause	$1,000-$50,000	$1.5 million
Willful Neglect, Corrected within 30 Days	$10,000-$50,000	$1.5 million
Willful Neglect, Not Corrected within 30 Days	$50,000	$1.5 million

The Final Rule also clarified that HHS will not impose the maximum penalty amount in all cases but will instead determine the penalty based on (i) the nature and extent of the violation; (ii) the resulting harm (*e.g.*, the number of individuals affected, reputational harm, etc.); (iii) the entity's history of prior offenses or compliance; (iv) the financial condition of the entity; and (v) any other factor that justice may require be considered. HHS also retains the ability to waive a CMP, in whole or in part, and to settle any issue or case or to compromise the amount of a CMP.

Finally, the Final Rule also included some much needed clarification regarding how HHS will count the number of violations and apply the tiered penalties (and the tiered penalty caps):

- Where multiple individuals are affected by an impermissible use or disclosure (such as in the case of a breach of unsecured protected health information) for purposes of levying penalties, the number of violations of the HIPAA Regulations will be based on the number of individuals affected. For example, if a breach involves the protected health information of 1,000 individuals, the breach will be viewed as 1,000 violations of the same provision.

- When a violation is continuous over a period of time (for instance, if a covered entity has inadequate technical safeguards in place over a period of time) for purposes of levying penalties, the number of identical violations will be based on the number of days in which the entity did not have adequate safeguards in place. For example, if an entity's technical safeguards are inadequate for 60 days, there will be 60 violations of the same provision.

- If an event involves violations of two provisions of the HIPAA Regulations (*e.g.*, there is an impermissible use or disclosure of protected health information and there are inadequate safeguards in place), HHS may calculate a separate CMP for each provision. This means that the annual penalty cap for such an event would be $3 million -- $1.5 million cap for the impermissible use or disclosure of protected health information plus the $1.5 million cap for inadequate safeguards.

HHS may also impose criminal penalties for certain wrongful disclosures. These criminal penalties can be enforced against covered entities, business associates, and individuals, including, but not limited to, employees of a covered entity or business associate. The criminal penalties vary depending on whether the offense is committed under false pretenses or with the intent to sell the information or use it for personal gain. Under HITECH, the maximum criminal penalties include fines up to $250,000 and up to 10 years imprisonment.

J. No Private Right of Action

Individuals do not have a private right of action under the HIPAA Regulations; that is, an individual may not sue under HIPAA for a violation of HIPAA. However, the HIPAA Regulations create a system which allows individuals to make complaints to OCR about potential violations, and the HIPAA Regulations require covered entities and business associates to develop a process to review complaints about such violations.[9]

K. State Laws

Separate from HIPAA and HITECH, there a number of state privacy and security laws that protect identifiable patient information, including information which is not health-related. Which state's laws are implicated is generally based on the state of the patient's residence. This Guide does not address state privacy and security laws in any detail. However, such laws are generally related to either special protections placed on specific types of health information (e.g., mental health records or information related to an individual's HIV/AIDS status) or providing notifications if an individual's personal information, including non-health-related information is disclosed or breached, particularly if such information is stored electronically.

In general, state laws that are contrary to the HIPAA Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply, unless the contrary state law provides more stringent protections to the privacy or security of the PHI than the HIPAA Regulations or the state law gives an individual greater rights with respect to the individual's PHI (e.g., a greater right to access PHI). In other words, the federal standards will not preempt a state law that is more stringent than the related federal requirements. In some instances, if federal and state requirements are not the same, but are not contrary to each other (i.e., compliance with one would result in the violation of the other), then both the state law and the federal law must be followed.

[9] While HITECH did not create a private right of action for violations of the HIPAA Regulations, it did include a section which would allow harmed individuals to benefit from and receive a portion of all CMPs and monetary settlements collected by OCR. As of the date of this publication, individuals do not have access to any percentage of such monies, as the implementing regulations for this requirement have not yet been finalized.

ATTACHMENT 1

PRIVACY POLICY AND PROCEDURES

I. INTRODUCTION

Because this office transmits patient records or information electronically, we are required to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the implementation regulations under both, including the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E (the "Privacy Rule") and the Security Standards for the Protection of Electronic PHI at 45 C.F.R. Parts 160, 162, and 164, Subparts A and C (the "Security Rule") (collectively, the "HIPAA Regulations"). HIPAA and the HIPAA Regulations apply to all protected health information (PHI) in the possession, custody, and control of this office – whether in electronic or paper form, or whether disclosed orally.

For purposes of this Privacy Policy, PHI includes any individually identifiable information, such as names, dates, phone/fax numbers, email addresses, home addresses, social security numbers, and demographic data. Employment records are not included within the definition (and thus not subject to the Privacy Policy) unless they are used in connection with the provision of treatment to the employee separate from such employee's employment.

II. PRIVACY OFFICER

_____ shall act as the Privacy Officer for this office unless another member of the office is formally appointed to serve as Privacy Officer. The Privacy Officer shall have overall responsibility for developing, establishing and maintaining this Privacy Policy, as well as developing any future amendments or revisions to this Privacy Policy.

The Privacy Officer shall also be responsible for receiving any complaints or inquiries about patient privacy matters, and responding to such complaints or inquiries. The Privacy Officer shall document all complaints or inquiries received. If any patient or other person desires to make a complaint relating to patient privacy, the Privacy Officer shall instruct him or her to submit the complaint in writing. The Privacy Officer shall then (i) investigate the complaint or inquiry; (ii) determine a resolution in conjunction with the doctor(s) in the office; and (iii) respond to the complainant or inquirer as to the results of the investigation and resolution.

If the inquiry is a complaint, the person shall be advised of his/her right to file a complaint with HHS within 180 days of the date of the alleged violation.

III. PRIVACY TRAINING

This office will routinely undertake privacy training for all staff. The training will occur on an annual basis for all existing staff, unless otherwise changed to a more frequent basis. In addition, all new staff shall participate in privacy training immediately upon their commencement of employment with this office. A written record of this training and an acknowledgment of the training will be maintained by the Privacy Officer.

IV. NOTICE AS TO USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Each patient shall be provided a Notice of Privacy Practices at their first appointment. *See* **Exhibit A**. A copy of the signed and dated Notice must be maintained in each patient's file. The Notice shall also be posted to the office's website (if applicable).

The Notice may be amended upon approval of the doctor(s) in the office. If the Notice is amended in a material way, the revised Notice must be made available to existing patients upon request and posted in the office. No material change to the Notice will be implemented prior to the effective date shown on the revised notice.

V. USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR TREATMENT PAYMENT AND HEALTH CARE OPERATIONS

This office may use PHI without the patient's Authorization for purposes of Treatment, Payment, or Healthcare Operations ("TPO"):

- *Treatment*. We may disclose PHI as necessary to provide treatment to a patient. For example, PHI may be disclosed to a referring doctor.

- *Payment.* We may disclose PHI as necessary to receive reimbursement or compensation for services provided. We may contact an insurer to get prior authorization or for billing purposes.

- *Healthcare Operations*. We may use PHI in patients' health records to carry out our health care operations, i.e., quality assessment and improvement activities, reviewing the competence of the qualifications of doctors, conducting training programs, and licensing and credentialing activities.

We may also share PHI with other covered entities and business associates who may have access to the PHI in the course of providing services to patients or to us.

Other Disclosures Permitted Without Authorization

There are other limited instances when we may use and disclose PHI without the patient's Authorization, provided that the patient has the opportunity to agree or object to the use or disclosure of all or part of the PHI. If the patient is not able to agree or object, we may use our professional judgment and determine if the disclosure is in the patient's best interest. In this

case, we may disclose only the PHI relevant to the patient's care. Anyone with questions regarding whether or not a disclosure is permitted should consult the Privacy Officer.

- *Others involved in a patient's healthcare*: Unless the patient objects, we may disclose to a member of the patient's family, a relative, close friend, or any other person the patient identifies, PHI that directly relates to that person's involvement in the patient's care or payment for that care. We may also disclose PHI to an authorized public or private entity to assist in disaster relief efforts and to coordinate disclosures to family or other individuals involved in the patient's care.

- *Notification*: We may disclose a patient's PHI to notify or assist in notifying a family member, personal representative, or another person responsible for the patient's care of the patient's location, general condition, or death.

VI. OTHER USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION NOT REQUIRING AUTHORIZATION

In addition to using and disclosing PHI for TPO (as described above), we may use and/or disclose PHI without a signed Authorization from the patient in the following situations:

- *As Required by Law:* to the extent that the use or disclosure is required by law, in compliance with the law, and limited to the relevant requirements of the law

- *Public Health:* for public health activities and purposes if the disclosure is to a public health authority permitted by law to collect or receive the information for the purpose of controlling disease, injury, or disability or, if directed by the public health authority, to a foreign government agency collaborating with the public health authority

- *Communicable Diseases:* (if authorized by law) to a person who may have been exposed to a communicable disease or otherwise at risk of contracting or spreading the disease or condition

- *Food and Drug Administration:* to a person or company required by the Food and Drug Administration (FDA) to report adverse events, product defects or problems, biologic product deviations, track FDA-regulated products, in order to enable product recalls, make repairs or replacements, or to conduct post marketing surveillance

- *Employers:* to an employer, about an individual who is a member of the employer's workforce, only under very limited circumstances as permitted by the Privacy Rule or required by law

- *Law Enforcement:* to a law enforcement official for law enforcement purposes, provided that certain conditions are met and only the permissible amount of PHI is disclosed, as is set forth in the relevant sections of the Privacy Rule

- *Health Oversight Activities:* to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations proceedings, or actions; inspections; licensure or disciplinary actions; or other activities necessary for appropriate oversight of the health care system

- *Judicial and Administrative Proceedings:* in response to an order of a court or administrative tribunal (provided that the order is signed by a judge) as expressly authorized by such order; or in response to a subpoena, discovery request, or other lawful process not accompanied by an order of a court or administrative tribunal only when we receive satisfactory assurances in accordance with the Privacy Rule that the patient has been notified of the request or efforts have been made to obtain an order protecting the requested PHI

- *To Avert a Serious Threat to Health or Safety:* when necessary to prevent a serious threat to a person's health or safety or the health or safety of the public when the disclosure is made to a person reasonably likely to prevent or lessen the threat, including the target of the threat; or when necessary for law enforcement authorities to identify or apprehend an individual

- *To Coroners, Funeral Directors, and for Organ Donation:* to a coroner or medical examiner for identification purposes, to determine cause of death, or for the coroner or medical examiner to perform other duties authorized by law; to a funeral director, as authorized by law, to permit the funeral director to carry out its duties; or to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for purposes of facilitating cadaveric organ, eye, or tissue donation

- *Research:* to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of PHI

- *Military:* as required by military command authorities to assure the proper execution of a military mission, if the appropriate military authority has published by notice in the Federal Register the appropriate military command authorities and the purposes for which the PHI may be used or disclosed

- *National Security and Intelligence Activities:* to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities authorized by the National Security Act and its implementing authority

- *Protective Services for the President and Others:* to authorized federal officials so they may provide protection to the President, other authorized persons, or foreign heads of state, or to conduct special investigations authorized by 18 U.S.C. § 871 and 879

- *Correctional Institution:* to a correctional institution or law enforcement officials having custody of an individual

- *Workers' Compensation:* as authorized by and to the extent necessary to comply with workers' compensation laws and other similar legally-established programs

- *Victims of Abuse, Neglect, or Domestic Violence:* under certain circumstances, in instances of child abuse, to a public health authority authorized by law to receive reports of child abuse or neglect; and in instances of abuse, neglect, or domestic violence (other than child abuse), to a government authority, such as a social service or protective services agency, authorized by law to receive reports of abuse, neglect, or domestic violence

- *Disclosures for HIPAA Compliance Investigations:* to the Secretary when so requested in connection with an investigation into our compliance with the HIPAA Regulations

Members of the office receiving a request for the use and disclosure of PHI, other than for TPO purposes or with a valid Authorization, should contact the Privacy Officer for approval.

VII. MINIMUM NECESSARY RULE

The use and disclosure of PHI must be limited to the "minimum necessary" to accomplish the purpose for which the use, disclosure, or request is made. Certain uses and disclosures are not subject to the "minimum necessary rule," including: disclosures to health care providers for treatment purposes, disclosures to the patient who is the subject of the PHI, disclosures made pursuant to the patient's authorization, uses or disclosures required for compliance with HHS, legal or law enforcement actions and disclosures required by law.

VIII. VERIFICATION

Members of this office must make reasonable efforts to verify the identity of the person with whom they are communicating to prevent disclosure of PHI to an unauthorized individual or entity. Members of the office may rely upon documentation, statements, or representations which appear on their face to meet the applicable HIPAA requirements, if such reliance is not unreasonable under the circumstances. If uncertain whether the requester is acting in good faith, a member of the office should consult the Privacy Officer. Verification is not required if the identity and authority of the requestor is known to the member(s) of the office.

IX. AUTHORIZATION TO USE AND DISCLOSE PATIENT INFORMATION

If a doctor in the office determines that PHI will be used or disclosed for any purpose other than in connection with treatment, payment or health care operations (defined above) or any other uses and disclosures permitted under the HIPAA Regulations, then the patient must sign our office-approved Authorization. *See* **Exhibit B**. For example, an Authorization would be appropriate where the patient's information will be disclosed to a potential employer to determine whether to hire the patient or making a disclosure of the information to a financial institution, marketing, etc.

If another Authorization form is presented to our office, it should be verified that the Authorization form complies with HIPAA (i.e., that it is written in plain language and contained at least the elements set forth in 45 C.F.R. § 164.508). If there is any question whether the Authorization complies with HIPAA, the Privacy Officer shall be consulted.

We may not accept Authorizations that are not valid (i.e., the expiration date has passed, the Authorization has not been filled out completely, any of the required elements are missing). A patient may revoke the Authorization in writing at any time.

X. BUSINESS ASSOCIATES

Any disclosure to business associates (as that term is defined under 45 C.F.R. § 160.103) (i.e., labs, collection agencies, attorneys, accountants, etc.) by this office may only occur after certain safeguards are in place. Namely, there must be a Business Associate Agreement (BAA) in place. *See* **Exhibit C**. The Privacy Officer will maintain a list of BAAs. A member of the office should consult the Privacy Officer before disclosing PHI to a third-party for purposes other than treatment and payment in order to ensure that an appropriate BAA is in place prior to the disclosure.

XI. MARKETING

Generally, members of the office should obtain a patient's Authorization to use and disclose the patient's PHI for purposes of marketing. If a communication encourages its recipient to purchase or use a product or service, it must be determined whether the communication falls under the definition of "marketing" found in 45 CFR § 164.501. If a communication meets the definition of marketing, we must obtain an Authorization from the patient, prior to making the marketing communication, unless the communication is in the form of (i) a face-to-face communication made by our office to a patient; or (ii) a promotional gift of nominal value provided by us.

XII. PATIENT RIGHTS

A. RIGHT TO REQUEST RESTRICTION ON USE AND DISCLOSURE

Patients may request restrictions on the use and disclosure of their protected health information. However, we are not obligated to honor these requests – except as provided below. If we elect to honor the request, we must adhere to it. Any denial must be in writing. If a patient asks us to restrict the disclosures of his/her PHI to a health plan made for payment and health care operations purposes and the PHI pertains solely to a health care item or service for which the patient (or someone acting on the patient's behalf) has paid us in full, we must agree to the restriction. While we are not required to create a separate medical record or otherwise segregate PHI subject to such a restriction, we need to flag or use some other method to identify portions of the record that contain PHI subject to the restriction in order to ensure it is not inadvertently sent or made accessible to the health plan.

B. RIGHT TO REQUEST CONFIDENTIAL COMMUNICATION OF PROTECTED HEALTH INFORMATION

Patients have the right to request confidential communication of their PHI. For example, they may request that the information be communicated by alternative means (i.e., sending correspondence to their office rather than to their home). If such a request is made, it should be in writing and we will abide by that request as long as it is reasonable. We are not allowed to inquire as to the reason(s) for the request.

C. RIGHT TO REQUEST ACCESS AND/COPIES OF THEIR RECORDS

Consistent with applicable ethics rules of the American Association of Orthodontists and the new privacy rules, we will provide patient records to them or their designee at any time. However, special permission from the doctor must be obtained prior to releasing the information if the information is compiled in anticipation of, or for use in, litigation or administrative (i.e., dental board) proceedings. (HIPAA does not require that the information be provided to the patient in those instances.) Any denial must be in writing.

If we maintain health information electronically in a designated record set, patients have a right to receive an electronic copy of their health information. If a patient makes such a request, we must provide the individual with access to the electronic information in the electronic form or format requested by the individual, if it is readily producible in the requested form or format – or in a form or format agreed to by both parties.

We have 30 days after receiving a request for access or copies from a patient within which to provide the access or information. A 30-day extension may be obtained if, within the initial 30-day period, we provide written notice to the patient of the reasons for the delay and give a date on which we will provide a response. We can charge the patient a "reasonable, cost-based fee" to provide the copy of the PHI.

D. TO AMEND OR MODIFY THEIR HEALTH INFORMATION

From time to time, patients may request that their protected health information be modified. Such a request must be made in writing. Generally, we will honor their requests. However, such requests will not be honored if the information is accurate and complete, or if we did not create the information.

If we honor the request, we must obtain a list of persons or entities that the patient wants us to inform of the amendment from the patient, along with the patient's authorization to inform them. We must then undertake reasonable efforts to notify those persons or entities of the amendment.

If we deny the request, the denial must be in writing and advise the patient of (1) the reasons for the denial, (2) their right to submit a "written disagreement", (3) his/her right to ask that the request to amend and our denial be included with any future disclosure of the subject information if not "written disagreement" is submitted, and (4) his/her right to file a complaint with the Secretary of HHS.

We must respond to any request to amend health information within 60 days of receiving the request. An additional 30 days is allowed if, within the original 60-day period, we notify the patient of the reason(s) for the delay and provide a date on which we will provide a response.

E. FOR AN ACCOUNTING OF DISCLOSURES

If requested and unless an exception exists, we will provide patients with a written accounting of all disclosures of their protected health information that we have made for the period requested, but not to exceed six years from the date of the request.

Unless decided otherwise by the doctor(s), we will not provide disclosures relating to the following:

1. Treatment of the patient, including disclosures made to other treatment providers (i.e., their general dentist, periodontist, etc.);

2. Payment by or on behalf of the patient;

3. Health Care Operations (i.e., information disclosed in connection with performance reviews, training, certification, accreditation or licensing);

4. Disclosures made to the patient or those involved in the care of the patient;

5. Incidental disclosures (i.e., from sign-up sheets, overheard conversations, etc.); or

6. Any disclosures that occurred pursuant to an Authorization signed by the patient.

We must respond to a patient's request for an accounting of disclosures within 60 days of the request. We can obtain an additional 30 days to respond by, within the initial 60-day period, providing the patient with written notice of the reason(s) for the delay and giving a date on which a response will be provided.

Patients are entitled to one free accounting within a 12-month period. Any further requests for an accounting of disclosures may involve a reasonable fee, which will be determined by the doctor(s) on a case-by-case basis and must be communicated to the patient at the time of the request.

XIII. ADMINISTRATIVE AND TECHNICAL SAFEGUARDS

This office will implement administrative, technical, and physical safeguards designed to protect against any use or disclosure of PHI in violation of this Privacy Policy or the HIPAA Regulations.

Administrative Safeguards

This office shall take measures reasonably designed to administratively safeguard the privacy of PHI. Such measures include but are not limited to developing this Privacy Policy and training employees and other office staff on the HIPAA Regulations. Employees and office staff are required to adhere to this Privacy Policy, and follow other established operational procedures for safeguarding PHI such as:

- Avoiding any action that might provide confidential information to an unauthorized individual or agency
- Refraining from reviewing or accessing records or files without a legitimate business need or without authorization
- Using pre-programmed fax numbers rather than dialing manually (to ensure the fax is going to the intended destination)
- Using pre-printed or computer-generated labels for mailing documents or packages whenever possible
- Using confidential files and data only for purposes specifically authorized
- Refraining from discussing with any unauthorized person, information or data that would lead to identification of individuals described in confidential files or data

Technical Safeguards

Members of the office shall take measures reasonably designed to technically safeguard the privacy of PHI used or maintained by this office. Such measures include but are not limited to:

- Using computer password and file access codes
- Not sharing access codes and passwords with others
- Not allowing unauthorized personnel access to files, computerized information, records or other confidential information/data

Physical Safeguards

Members of this office shall take measures reasonably designed to physically safeguard the privacy of PHI. Such measures include, but are not limited to:

- Taking reasonable precautions so that PHI is not visible or audible to passers-by
- Taking precautions to store or cover documents containing PHI when walking away from a desk or work area

- Storing documents with PHI in locked file cabinets or in areas to which access is restricted

- Using standardized cover sheets when faxing PHI

- Clearly marking "Confidential" and maintaining in a secured area any documents containing PHI in storage, whether on or off-site

- Shredding or otherwise destroying labels, documents, disks or any other media containing PHI prior to disposal in accordance with the section on Disposal of Protected Health Information

- Never taking PHI off-site, except as authorized in the performance of job duties

- Taking care that any PHI, whether in paper or electronic format, is physically and technologically secure when it is taken off-site in connection with authorized off-site job duties

- Applying password protection to personal data devices used to store or transmit PHI

XIV. REPORTING AND INVESTIGATING SUSPECTED VIOLATIONS

All members of this office are expected to report actual or suspected violations of the HIPAA Regulations or this Privacy Policy to the Privacy Officer who will investigate any allegation of a HIPAA violation and take any corrective actions.

If a member of the office suspects or knows that this Policy or the HIPAA Regulations have been violated by another employee or contractor, the employee or contractor is required to report the actual or suspected violation, preferably in writing, to the Privacy Officer. If the alleged violation involves the Privacy Officer, it shall be reported to a doctor in the office. A member of the office may submit anonymous allegations if they wish, but identification facilitates the office investigation. Every effort will be made to protect the confidentiality of these communications to the extent possible and ensure that no threats or retaliations occur against any member of the office making an allegation in good faith. Anyone who threatens or retaliates against any member of the office who reports a potential violation of the regulations or our policies or procedures is subject to disciplinary action, up to and including termination.

XV. NOTIFICATION OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION

If any member of the office becomes aware of any actual or suspected unauthorized use or disclosure of unsecured PHI (i.e., unencrypted PHI), he/she must immediately notify the Privacy Officer. The Privacy Officer will immediately take steps to determine if there has been a breach (as that term is defined by 45 CFR § 164.402), and if there has been a breach, to mitigate any

harmful effects of the breach and initiate notification procedures in accordance with the HIPAA, the HIPAA Regulations and HITECH.

XVI. RECORD RETENTION

This office shall create documentation of compliance activities as described in this Privacy Policy and as required by HIPAA, the HIPAA Regulations, and HITECH. Documentation required or generated by this office in accordance with this Privacy Policy (i.e., this Privacy Policy, signed and dated Authorizations, Notice of Privacy Practices and breach notification letters) shall be retained for a period of six (6) years from the later of the date of creation or law use, unless state or federal law requires a longer retention period.

XVII. DISPOSAL OF PROTECTED HEALTH INFORMATION

This office's PHI may only be disposed of by means that ensure that it will not be accidentally released to an outside party. PHI must not be discarded in unsecured or open trash bins, unsecured recycle bags, or other publicly accessible locations, and may only be placed in a secured bag or box for delivery to a shredding service; and printed material and electronic data containing PHI shall be disposed of in a manner that ensures confidentiality. It is the responsibility of each member of the office granted access to PHI to ensure that any documents, packages, or electronic media containing PHI have been secured or destroyed.

XVIII. VIOLATION OF PRIVACY POLICY / SANCTIONS

This office takes seriously the need to fully comply with the HIPAA Regulations and has a commitment to protecting confidential healthcare information. Any violation of this Privacy Policy shall be grounds for discipline, including termination. Compliance with this Policy is required in addition to all other office personnel policies, if any.

All members of this office must be familiar with this Privacy Policy and abide by the requirements set forth herein. Questions about this Privacy Policy should be directed to the Privacy Officer.

Exhibit A

NOTICE OF PRIVACY PRACTICES

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

UNDERSTANDING YOUR HEALTH INFORMATION

Each time you visit our office, we make a record of your visit in order to manage the care you receive. We understand that the medical information that is recorded about you and your health is personal. The confidentiality and privacy of your health information is also protected under both state and federal law.

This Notice of Privacy Practices describes how this office may use and disclose your information and the rights that you have regarding your health information.

How We Will Use or Disclose Your Health Information

Treatment: We will use your health information for treatment. For example, information obtained by the orthodontist or other members of your healthcare team will be recorded in your record and used to determine the course of treatment that should work best for you. Your orthodontist will document in your record his or her expectations of the members of your healthcare team. Members of your healthcare team will then record the actions they took and their observations, so the physician will know how you are responding to treatment. We will also provide your physician, or a subsequent healthcare provider, with copies of various reports that should assist him or her in treating you.

Payment: We will use your health information for payment. For example, a bill may be sent to you or your health plan. The information on or accompanying the bill may include information that identifies you, as well as your diagnosis, procedures, and supplies used.

Health Care Operations: We will use your health information for our regular health care operations. For example, we may use information in your health record to assess the care and outcome in your case and others like it. This information will then be used in a continued effort to improve the quality and effectiveness of the services we provide.

Business Associates: We may enter into contracts with persons or entities known as business associates that provide services to or perform functions on our behalf. Examples include our accountants, consultants, and attorneys. We may disclose your health information to our business associates so they can perform the job we have asked them to do, once they have agreed in writing to safeguard your information.

Notification: We may use or disclose information to assist in notifying a family member, personal representative, or another person responsible for your care, of your location, and general condition. If we are unable to reach your family member or personal representative, then we may leave a message for them at the phone number that they have provided to us, e.g., on an answering machine.

Communication with Family: We may disclose to a family member, other relative, close personal friend or any other person you identify, health information relevant to that person's involvement in your care or payment related to your care.

Appointment Reminders / Health Benefits: We may contact you to provide appointment reminders or information about treatment alternatives or other health benefits that may be of interest to you.

Funeral Directors and Coroners: We may disclose your health information to funeral directors, and to coroners or medical examiners, to carry out their duties consistent with applicable law.

Organ Procurement Organizations: Consistent with applicable law, we may disclose your health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for the purpose of tissue donation and transplant.

Research: We may disclose your health information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your health information. We may also disclose your health information to people preparing to conduct a research project, so long as the health information is not removed from us. We may also use and disclose your health information to contact you about the possibility of enrolling in a research study.

Fundraising: We may contact you as part of our fundraising efforts; however, you may opt-out of receiving such communications.

Food and Drug Administration (FDA): We may disclose to the FDA health information relative to adverse events with respect to food, supplements, product, and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacement.

Workers' Compensation: We may disclose health information to the extent authorized by and to the extent necessary, to comply with laws relating to workers' compensation or other similar programs established by law.

Public Health Activities: As required by law, we may disclose your health information to public health, or legal authorities, charged with preventing or controlling disease, injury, or disability.

Health Oversight Activities: We may disclose your health information to health oversight agencies for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.

Correctional Institution: Should you be an inmate of a correctional institution, we may disclose to the institution, or agents thereof, health information necessary for your health and the health and safety of other individuals.

Judicial and Administrative Proceedings: We may disclose your health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.

Law Enforcement Purposes / Serious Threat to Health or Safety: We may disclose your health information to enforcement officials for law enforcement purposes under certain circumstances and subject to certain conditions. We may also disclose your health information to prevent or lessen a serious and imminent threat to a person or the public (when the disclosure is made to someone we believe can prevent or lessen the threat) or to identify or apprehend an escapee or violent criminal.

Victims of Abuse, Neglect, and Domestic Violence: In certain circumstances, we may disclose your health information to appropriate government authorities if there are allegations of abuse, neglect, or domestic violence.

Essential Government Functions: We may disclose your health information for certain essential government functions (e.g., military activity and for national security purposes).

The following uses and disclosures will be made only with your authorization: (i) with limited exceptions, uses and disclosures of your health information for marketing purposes, including subsidized treatment communications; (ii) disclosures that constitute a sale of your health information; and (iii) other uses and disclosures not described in this notice. You may revoke your authorization at any time in

writing, except to the extent that we have taken action in reliance on the use or disclosure indicated in the authorization.

Your Health Information Rights

Although your health record is the physical property of this office, you have the following rights with respect to your health information:

- You may request that we not use or disclose your health information for a particular reason related to treatment, payment, our general healthcare operations, and/or to a particular family member, other relatives or close personal friend. We ask that such requests be made in writing on a form provided by us. Although we will consider your request, please be aware that we are under no obligation to accept it or to abide by it, except as provided below.

- If you have paid for services out-of-pocket in full, you may request that we not disclose information related solely to those services to your health plan. We ask that such requests be made in writing on a form provided by us. We are required to abide by such a request, except where we are required by law to make a disclosure. We are not required to inform other providers of such a request, so you should notify any other providers regarding such a request.

- You have the right to receive confidential communications from us by alternative means or at an alternative location. Such a request must be made in writing, and submitted to the Privacy Officer. We will attempt to accommodate all reasonable requests.

- You may request to inspect and/or obtain copies of health information about you, which will be provided to you in the time frames established by law. If we maintain your health information electronically in a designated record set, you may obtain an electronic copy of the information. If you request a copy (paper or electronic), we will charge you a reasonable, cost-based fee.

- If you believe that any health information in your record is incorrect, or if you believe that important information is missing, you may request that we correct the existing information or add the missing information. Such requests must be made in writing, and must provide a reason to support the amendment. We ask that you use the form provided by us to make such requests. For a request form, please contact the Privacy Officer.

- You may request that we provide you with a written accounting of all disclosures made by us during the time period for which you request (not to exceed six years), as required by law. We ask that such requests be made in writing on a form provided by us. Please note that accounting does not include all disclosures, e.g., disclosures to carry out treatment, payment, or healthcare operations and disclosures made to you or your legal representative or pursuant to an authorization. You will not be charged for your first accounting request in any 12-month period. However, for any requests that you make thereafter, you will be charged a reasonable, cost-based fee.

- You have the right to be notified following a breach of your unsecured protected health information.

- You have the right to obtain a paper copy of our Notice of Privacy Practices upon request.

For More Information or to Report a Problem

You have the right to complain to us and to the Secretary of the U.S. Department of Health and Human Services (HHS) if you believe we have violated your privacy rights. We will not retaliate against you for filing a complaint.

For more information or to file a complaint with us, contact our Privacy Officer by phone or mail as follows:_____. To file a complaint with the Secretary of HHS, send your complaint to: **[INSERT ADDRESS FOR REGIONAL OFFICE OF OFFICE OF CIVIL RIGHTS]**

If you have any questions or want more information about this Notice of Privacy Practices, please contact our Privacy Officer.

Acknowledged By: _____ Date: _____
Signature of Patient or Personal Representative

[INSERT EFFECTIVE DATE OF THE NOTICE]

Exhibit B

PATIENT AUTHORIZATION FOR SPECIFIC DISCLOSURE OF PROTECTED HEALTH INFORMATION

I, the undersigned, hereby authorize [INSERT PROVIDER NAME] to disclose certain protected health information about me to:

_____

(Name) (Address)

[INSERT PROVIDER NAME] is hereby authorized to disclose the following protected health information (specifically describe the information to be disclosed, such as date(s) of services, type of services, level of detail to be released, origin of information, etc.):

☐ All Medical Records ☐ x-Rays ☐ Specific Information Listed Below:

_____

_____

_____

I understand that this request does not apply to: (1) certain health information that is not held in [INSERT PROVIDER NAME]'s medical records; (2) psychotherapy notes; (3) information compiled in reasonable anticipation of or for litigation; and (4) other health information not subject to the right of access under HIPAA.

The information may be disclosed for the following purpose:

_____

_____

This authorization will expire 90 days after the date of its execution or on_____ (name specific date or event), unless expressly revoked by me at an earlier time.

I understand that [INSERT PROVIDER NAME] may not condition my treatment on whether I sign this authorization.

I understand that if my protected health information is disclosed to someone who is not required to comply with the federal HIPAA regulations, then such information may be re-disclosed by the recipient and may no longer be protected by HIPAA.

I understand that I may revoke this authorization at any time by delivering a revocation in writing to [INSERT PROVIDER NAME] at the address listed above, and if I revoke this authorization, it will have no effect on actions already taken by [INSERT PROVIDER NAME] in reliance on this authorization.

I authorize the disclosure described herein. I have read and understand this authorization. I am the patient listed on this authorization or am authorized to act on behalf of the patient as the patient's personal representative.

Signature of Patient or Legal Guardian:_____ Date:_____

Patient Name: _____ SS# _____

Address:_____ City:_____ State: ____ Zip_____

DOB:_____ Phone:_____

Printed Name of Patient or Legal Guardian:_____

Witness:_____

PATIENT/GUARDIAN TO BE PROVIDED WITH A SIGNED COPY OF AUTHORIZATION

Exhibit C

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is effective as of _____ and is by and between _____ ("Covered Entity") and _____ ("Business Associate").

RECITALS

A. Covered Entity and Business Associate are parties to an agreement or arrangement pursuant to which Business Associate performs certain services for Covered Entity.

B. In connection with the performance of its services, Business Associate may receive from, or create or receive on behalf of Covered Entity health information that is considered PHI (as defined below).

C. To the extent that such PHI is shared between the parties, this Agreement shall apply and shall set forth the party's obligations with respect to such PHI.

D. The provisions of this Agreement shall become binding on the parties beginning on the date on which PHI is first shared between the parties and shall terminate in accordance with the terms of this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the parties agree as follows:

TERMS

1. **Definitions**

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Rules (as defined below), the HITECH Standards (as defined below) or any future regulations promulgated or guidance issued by the Secretary (as defined below) thereunder.

(i) Breach. "Breach" shall have the same meaning as the term "breach" at 45 C.F.R. § 164.402.

(ii) Designated Record Set. "Designated Record Set" shall mean a group of records maintained by or for a covered entity that is:

- The Medical Records & Billing Records of a patient/individuals for a Covered Entity.
- Enrollment, payment, claims adjudication, and case or medical management records systems maintained by a Health Plan.
- Used by the covered entity to make decisions about patients/ individuals, in whole or in part.

The term "record" refers to any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

(iii) Electronic Health Record. "Electronic Health Record" shall mean an electronic record of health-related information on an Individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

(iv) Electronic PHI. "Electronic PHI" shall have the same meaning as the term "electronic PHI" at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(v) HIPAA. "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, as amended, and the implementation regulations thereunder, including without limitation the HIPAA Rules (as defined below) and the HITECH Standards (as defined below), and all future regulations promulgated thereunder.

(vi) HIPAA Rules. "HIPAA Rules" means the Privacy Rule (as defined below) and the Security Rule (as defined below).

(vii) HITECH Standards. "HITECH Standards" means Subtitle D of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), found at Title XIII of the American Recovery and Reinvestment Act of 2009, and any regulations promulgated thereunder, including all amendments to the HIPAA Rules.

(viii) Individual. "Individual" shall have the same meaning as the term "individual" at 45 C.F.R. § 160.103, and any amendments thereto, and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

(ix) Privacy Rule. "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164.

(x) Protected Health Information. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" at 45 C.F.R. § 160.103, and any amendments thereto, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(xi) Required By Law. "Required By Law" shall have the same meaning as the term "required by law" at 45 C.F.R. § 164.103.

(xii) Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

(xiii) Security Incident. "Security Incident" shall have the same meaning as the term "security incident" at 45 C.F.R. § 164.304.

(xiv) Security Rule. "Security Rule" shall mean the Security Standards for the Protection of Electronic PHI at 45 C.F.R. Parts 160, 162, and 164.

(xv) Unsecured PHI. "Unsecured PHI" shall have the same meaning as the term "unsecured protected health information" at 45 C.F.R. § 164.402.

2. **Relationship of Parties**

In the performance of the work, duties and obligations described in this Agreement or under any other agreement between the parties, the parties acknowledge and agree that each party is at all times acting and performing as an independent contractor and at no time shall the relationship between the parties be construed as a partnership, joint venture, employment, principal/agent relationship, or master/servant relationship.

3. **Ownership of PHI**

Business Associate acknowledges that all right, title and interest in and to any PHI furnished to Business Associate vests solely and exclusively with Covered Entity or the Individual to whom such PHI relates.

4. **Obligations and Activities of Business Associate**

(i) Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement, any underlying agreement between the parties, or as Required By Law.

(ii) Business Associate will make reasonable efforts, to the extent practicable, to limit requests for and the use and disclosure of PHI to a Limited Data Set (as defined in 45 C.F.R. § 164.514(e)(2)) or, if needed by Business Associate, to the minimum necessary PHI to accomplish the intended purpose of such use, disclosure or request, and as applicable, in accordance with the regulations and guidance issued by the Secretary on what constitutes the minimum necessary for Business Associate to perform its obligations to Covered Entity under this Agreement, any underlying agreement, or as Required By Law.

(iii) Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement.

(iv) Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI that it creates,

receives, maintains, or transmits on behalf of Covered Entity. Business Associate shall comply with the applicable requirements of the Security Rule in the same manner such provisions apply to Covered Entity.

(v) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

(vi) Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which it becomes aware. To the extent that Business Associate creates, receives, maintains or transmits Electronic PHI, Business Associate agrees to report as soon as practicable to Covered Entity any Security Incident, as determined by Business Associate, involving PHI of which Business Associate becomes aware. Notwithstanding the foregoing, Business Associate and Covered Entity acknowledge the ongoing existence and occurrence of attempted but unsuccessful Security Incidents that are trivial in nature, such as pings and port scans, and Covered Entity acknowledges and agrees that no additional notification to Covered Entity of such unsuccessful Security Incidents is required. However, to the extent that Business Associate becomes aware of an unusually high number of such unsuccessful Security Incidents due to the repeated acts of a single party, Business Associate shall notify Covered Entity of these attempts and provide the name, if available, of said party. At the request of Covered Entity, Business Associate shall identify the date of the Security Incident, the scope of the Security Incident, Business Associate's response to the Security Incident, and the identification of the party responsible for causing the Security Incident, if known.

(vii) Following Business Associate's discovery of a Breach of Unsecured PHI, Business Associate shall notify Covered Entity of the Breach without unreasonable delay, and in no event later than three (3) business days after Business Associate, or any of its employees or agents, discovered the Breach. Such notification shall include, to the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during the Breach and any other information available to Business Associate about the Breach which is required to be included in the notification of the Breach provided to the Individual in accordance with 45 C.F.R. §164.404(c). A Breach of Unsecured PHI shall be treated as discovered as of the first day on which such Breach is known to Business Associate or should have been known to Business Associate by exercising reasonable diligence. If Business Associate (or one of its subcontractors, vendors or agents) is responsible for a Breach of Unsecured PHI, Covered Entity may, at its option, require Business

Associate to provide any of the notifications required by 45 C.F.R. § 164.404 at Business Associate's expense.

(viii) In accordance with 45 C.F.R. §§ 164.308(b)(2) and 164.502(e)(1)(ii), Business Associate agrees to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree in writing to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Moreover, Business Associate agrees to ensure any such agent or subcontractor agrees to implement reasonable and appropriate safeguards to protect Covered Entity's Electronic PHI.

(ix) Business Associate shall provide access, at the request of Covered Entity, and in a time and manner mutually acceptable to Business Associate and Covered Entity, to PHI in a Designated Record Set to Covered Entity, or, as directed by Covered Entity, to an Individual or another person properly designated by the Individual, in order to meet the requirements under 45 C.F.R. § 164.524. If Business Associate maintains PHI electronically in a Designated Record Set and if the Individual requests an electronic copy of such information, Business Associate must provide Covered Entity, or the Individual or person properly designated by the Individual, as directed by Covered Entity, access to the PHI in the electronic form and format requested by the Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual. Any fee that Business Associate may charge for such electronic copy shall not be greater than Business Associate's labor and supply costs in responding to the request.

(x) Business Associate agrees to make any amendment(s) to PHI in its possession contained in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Covered Entity or an Individual, and in a time and manner mutually acceptable to Business Associate and Covered Entity.

(xi) Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. As of the compliance date set forth in the regulations promulgated under HITECH or as otherwise determined by the Secretary, in addition to the accounting of disclosure obligations required under 45 C.F.R. § 164.528, Business Associate shall account for all disclosures of PHI made through an Electronic Health Record in accordance with the HITECH Standards and any future regulations promulgated thereunder.

(xii) Within ten (10) business days (or such other date that Business Associate and Covered Entity may reasonably agree upon) of receiving written

notice from Covered Entity that Covered Entity has received a request for an accounting of disclosures of PHI, Business Associate agrees to provide to Covered Entity information collected to permit Covered Entity to make the accounting required in accordance with 45 C.F.R. § 164.528.

(xiii) Business Associate shall make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary for purposes of determining Covered Entity's or Business Associate's compliance with the Privacy Rule.

(xiv) To the extent Business Associate is to carry out Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such delegated obligation.

5. **General Use and Disclosure Provisions**

Except as otherwise limited in this Agreement:

(i) Business Associate reserves the right to **use** PHI for the proper management and administration of Business Associate, to carry out the legal responsibilities of Business Associate, and to provide data aggregation services to Covered Entity.

(ii) Business Associate may **use or disclose** PHI to perform functions, activities, or services for, or on behalf of, Covered Entity provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

(iii) Business Associate may **disclose** PHI in its possession for the proper management and administration of Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the third party to whom the information is disclosed that such PHI will be held confidentially and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the third party, and the third party notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

6. **Indemnification, Settlement and Procedure**

Notwithstanding any agreement by the Parties to the contrary, Business Associate shall indemnify and hold harmless Covered Entity and its directors, officers, affiliates, agents, volunteers, trustees or employees from and against any claim, cause of action, liability, damage, cost or expense, including attorney's fees and court or proceeding costs, arising out of or in connection with Business Associate's material breach of its obligations under this Agreement, as well as any violation of or failure of Business Associate to fulfill its obligation under HIPAA, including the unauthorized use or disclosure of PHI, or any failure in security measures affecting PHI by the Business Associate, its subcontractors, vendors or agents, or any person or entity under the Business Associate's control. The Business Associate's obligation to indemnify Covered Entity in accordance with this Section will survive expiration or termination of this Agreement. Covered Entity may, at its option, conduct its defense or settlement of any such action arising as described herein, and Business Associate shall cooperate with such defense and settlement.

7. **Term and Termination**

(i) Term. The term of this Agreement shall commence on the Effective Date, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is not feasible to return or destroy the PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

(ii) Termination for Cause. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or

(2) Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.

Business Associate shall ensure that it maintains the termination rights in this Section in any agreement it enters into with a subcontractor pursuant to Section 4(h) hereof.

(iii) Effect of Termination.

(1) Except as provided in paragraph (ii) of this Section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered

Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall not retain copies of the PHI.

(2) In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction not feasible. Upon determination that return or destruction of PHI is not feasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction not feasible, for so long as Business Associate maintains such PHI.

8. **Miscellaneous**

(i) Regulatory References. A reference in this Agreement to a section in the Privacy Rule or the Security Rule means the section as in effect or as amended and for which compliance is required.

(ii) Amendment. No change, amendment, or modification of this Agreement shall be valid unless set forth in writing and agreed to by both parties. Notwithstanding the foregoing, the parties acknowledge that state and federal laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Agreement may be required to ensure compliance with such developments. The parties specifically agree to take such action as may be necessary from time to time for the parties to comply with the requirements of HIPAA. Covered Entity shall provide written notice to Business Associate to the extent that any final regulation or amendment to final regulations promulgated by the Secretary under HITECH requires an amendment to this Agreement to comply with HIPAA. The parties agree to negotiate an amendment to the Agreement in good faith; however, either party may terminate this Agreement upon ninety (90) days written notice to the other party if the parties are unable to reach an agreement.

(iii) Survival. The respective rights and obligations of Business Associate under Section 7 of this Agreement shall survive the termination of this Agreement, unless expressly stated otherwise.

(iv) Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity and Business Associate to comply with HIPAA.

(v) Notice. Any notice, report or other communication required under this Agreement shall be in writing and shall be delivered personally, telegraphed, emailed, sent by facsimile transmission, or sent by U.S. mail.

(vi) Governing Law. The rights, duties and obligations of the parties to this Agreement and the validity, interpretation, performance and legal effect of this Agreement shall be governed and determined by applicable federal law with respect to the Privacy Rule and the Security Rule and otherwise by the laws of **[INSERT STATE].**

(vii) Counterparts. This Agreement may be executed in one or more original counterparts and will become operative when each party has executed and delivered at least one counterpart. Each original counterpart will be deemed to be an original for all purposes, and all counterparts will together constitute one instrument.

(viii) Signatures. This Agreement may be signed electronically and delivered by email, facsimile or similar transmission, and an email, facsimile or similar transmission evidencing execution, including PDF copies of executed counterparts, will be effective as a valid and binding agreement between the Parties for all purposes.

IN WITNESS THEREOF, each party has caused this Agreement to be executed by its duly authorized representative.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
Name	Name
Authorized Signature	Authorized Signature
Title	Title
Date	Date