CHILDREN'S DENTISTRY OF AMARILLO

HIPAA MANUAL

February 16, 2026

Prepared by:

Denise Leard, Esq.
Phuong Nguyen, Esq.
Brown & Fortunato, P.C.
701 S. Fillmore, Suite 400
Amarillo, Texas 79101
(806) 345-6300
www.bf-law.com

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

TABLE OF CONTENTS

INTRODUCTION

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was the first comprehensive federal legislation regarding confidentiality of patient medical records. The purpose of HIPAA is to improve the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of health information, most specifically the Privacy Standards and the Security Standards. The Privacy Standards provides for the protection of an individual's PHI by limiting uses or disclosures of personal health information (PHI) without proper authorization. In turn, the Security Standards addresses the protection of PHI, particularly electronic PHI, through administrative, physical and technical safeguards. For example, it sets forth the standards, procedures and methods for securing PHI with attention to how PHI is stored, accessed, transmitted, audited and destroyed. Use of emails, laptops, computers and cell phones should be conducted in compliance with HIPAA. These protections are given to all consumers regardless of whether they are privately insured, uninsured, or participants in public programs such as Medicare or Medicaid.

HIPAA also allows consumers to have more control over their private health information. It allows consumers to make informed choices related to how their PHI may be used. For health care providers, HIPAA requires the provider to, among other things:

1. Provide information to individuals about their privacy rights and how their information can be used;

2. Adopt clear privacy procedures;

3. Train its employees so that they understand the privacy procedures;

4. Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed: and

5. Secure records containing PHI so that PHI is not readily available to those who do not need it.

HIPAA and its standards continue to be amended from time to time. For example, the Health Information Technology for Economic and Clinical Health Act (HITECH), which was enacted as part of the American Recovery and Reinvestment Act of 2009, made significant changes to the privacy and security provisions of HIPAA. Another example is the Genetic Information Nondiscrimination Act of 2008 (GINA) which clarifies that genetic information is protected under the HIPAA Privacy Rule and prohibits most health plans from using or disclosing genetic information for underwriting purposes.

HIPAA and its standards establish only a federal floor of safeguards to protect the confidentiality of medical information. In circumstances where the federal rules and state laws are in conflict, the law which provides a stronger protection of privacy prevails. Thus, it is important to be aware of

Children's Dentistry of Amarillo's (hereinafter the "Practice") obligations under state dental privacy laws as well as under HIPAA and federal regulations.

Overview of This Manual

This Manual is a comprehensive guide detailing federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) and compliance with specific HIPAA regulations. Specifically, the first 61 pages of the Manual provide a detailed explanation of HIPAA's legal requirements, including the application of HIPAA; administrative requirements; individual rights under HIPAA; authorizations; use and disclosures of protected health information (PHI); and HIPAA security standards. At the end of the Manual, pages 62 through 153 provide Exhibits, listed A through Z, of sample forms and sample policies and procedures for implementing a HIPAA Compliance Program. The Exhibits include policy and procedures for Privacy and Security Standards as well as sample forms for Notice of Privacy Practices, Authorization to Release PHI, and Business Associate Agreements. These policies and forms may be revised and adopted by Children's Dentistry of Amarillo as the entity deems appropriate for its operations.

APPLICATION OF HIPAA

The basic privacy requirement of HIPAA is that a covered entity or business associate may not use or disclose an individual's PHI except with the individual's authorization, or as otherwise permitted or required by HIPAA. HIPAA's coverage applies only to PHI. However, the HIPAA definitions of covered entity, business associate, and PHI are very broad. As a result, many entities must comply with HIPAA and a wide variety of information is considered PHI.

Are You a Covered Entity?

Covered entities are:

1. Health care providers that transmit health information in electronic form in connection with covered transactions;

2. Health plans; and

3. Health care clearinghouses.

A health care provider is a provider of medical or health services and any other person or organization that furnishes, bills, or is paid for, health care in the normal course of business. Dentists fit within the definition of health care provider. A health care provider is a covered entity for purposes of HIPAA if the health care provider electronically transmits health information in any of the following transactions:

1. Health care claims or equivalent encounter information;

2. Health care payment and remittance advices;

3. Coordination of benefits;

4. Health care claim status;

5. Enrollment and disenrollment in a health plan;

6. Eligibility for a health plan;

7. Health plan premium payments;

8. Referral certification and authorization;

9. First report of injury;

10. Health claims attachment;

11. Health care electronic funds transfers and remittance advice; or

12. Other transactions that may be prescribed by regulation.

A provider is a covered entity if it submits claims to a payor electronically**.** Nearly all health care providers are required to submit claims electronically and, therefore, are covered entities. All PHI maintained by a covered entity must be protected. This includes not only information that is stored electronically, but also information that is verbal or written.

Are You A Business Associate?

A business associate includes a person or entity that "*creates, receives, maintains, or transmits*" PHI on behalf of a covered entity but other than in the capacity of a member of the workforce of such covered entity. In addition, a business associate may be a person or entity that provides, other than in the capacity of a member of the workforce of such covered entity, services, functions or activities to or for such covered entity, where the provision of the service involves the disclosure of PHI from such covered entity, or from another business associate of such covered entity or arrangement, to such person or entity. The HIPAA regulations specifically include subcontractors that create, receive, maintain, or transmit PHI on behalf of a business associate to be business associates themselves. In addition, a covered entity may be a business associate of another covered entity.

Covered entities often contract with other entities to perform health care activities and functions. In order for a business associate to carry out its functions, it is often necessary for a covered entity to release PHI to the business associate. A covered entity may only release PHI to a business associate to help the covered entity perform and carry out health care operations. PHI may not be used by the business associate for its own purposes.

HIPAA requires a covered entity to obtain assurances that the business associate will safeguard the PHI from misuse and will help the covered entity comply with the covered entity's duties to provide individuals with access to health information about them and a history of disclosures. This is generally accomplished through the use of a Business Associate Agreement or a Business Associate Addendum to the services agreement between the parties. A sample Business Associate Agreement and sample Business Associate Addendum are attached as Exhibits L1 and L2, respectively. This requirement does not mean that the covered entity must actively monitor or oversee the means by which the business associate carries out safeguards or the extent to which the business associate abides by the requirements of the Business Associate Agreement. However, if a covered entity becomes aware of a practice by the business associate that is a breach of the business associate's obligations, the covered entity must take reasonable steps to cure the breach or the covered entity must end the relationship.

Business associates of covered entities are directly liable for compliance with most of the HIPAA Privacy and Security Standards' requirements. Business associates are directly liable under the HIPAA Rules for: (i) impermissible uses and disclosures; (ii) failure to provide breach notification to the covered entity; (iii) failure to provide access to a copy of electronic PHI to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement); (iv) failure to disclose PHI where required by the Secretary to investigate or determine

the business associate's compliance with the HIPAA Rules; (v) failure to provide an accounting of disclosures, and (vi) failure to comply with the requirements of the Security Rule. Business associates also remain contractually liable for other requirements of the business associate agreement. In addition, civil and criminal penalties also apply to business associates directly.

A policy and procedure related to business associates is attached as Exhibit L3.

What Information Must Be Protected?

The Privacy Standards apply to PHI, which is defined as "individually identifiable health information" held or transmitted by a covered entity or its business associate in any form or media, whether electronic, paper, or oral. PHI is any information that is created or received by a covered entity or its business associate and that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, **if** the information identifies the individual or could be used to identify the individual. PHI does not include individually identifiable health information of persons who have been deceased for more than 50 years or individually identifiable health information contained in employment records held by a covered entity in its role as an employer.

PHI includes a wide variety of information. A provider's intake documents generally contain information related to the individual's past and present medical condition. In addition, insurance plan documentation requirements make it necessary for a provider to obtain as much information as possible to support medical necessity. Dental and other medical records, including records from a previous treating dentist, are clearly related to the past, present or future physical condition of an individual, and therefore these documents are considered PHI.

ADMINISTRATIVE REQUIREMENTS

Privacy Official

Each covered entity is required to designate a privacy official who is responsible for the development and implementation of the privacy policies and procedures of the covered entity. A covered entity must also designate a contact person or office that is responsible for receiving complaints and that is able to provide further information about matters covered by the Notice of Privacy Practices.[1] For most covered entities, this is the same individual.

The Privacy Officer's chief responsibilities should include:

1. Being involved in the development of policies and procedures necessary for HIPAA compliance, in coordination with the entity's management and administration, privacy committee, and legal counsel;

2. Performing initial and periodic privacy risk assessments;

3. Ensuring that the Notice of Privacy Practices, Authorization, Acknowledgment, and other materials reflecting the entity's privacy practices are compliant with HIPAA;

4. Ensuring delivery of initial and periodic privacy training to all employees, medical and professional staff, contractors, and other appropriate third parties;

5. Reviewing all contracts with business associates to ensure that HIPAA requirements are being met;

6. Establishing mechanisms to track access to PHI;

7. Being responsible for ensuring the entity does not infringe upon an individual's right to inspect, amend, and restrict access to PHI when appropriate;

8. Establishing and administering a process for receiving, documenting, tracking, investigating, and responding to all complaints concerning the entity's privacy policies and procedures;

9. Ensuring compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the entity's workforce;

---

[1] Section 164.520 of the Privacy Standards requires each covered entity to provide individuals with written notice of the uses and disclosures of PHI that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to PHI. This notice is usually referred to as a Notice of Privacy Practices. The Notice of Privacy Practices is discussed in more detail elsewhere in this Manual.

10. Being aware of applicable federal and state privacy laws and accreditation standards;

11. Cooperating with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations; and

12. Working with the entity's administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) that undertake to adopt or amend privacy legislation, regulation or standard.

An effective Privacy Officer should have enough authority within the office to get things done and to enforce the required procedures. The designation of the Privacy Officer shall be documented and maintained in the Practice's records.

Training

A covered entity must train all of its employees on the policies and procedures with respect to PHI as necessary and appropriate for the members of the workforce to carry out their responsibilities. HIPAA requires all covered entities to document the training provided to its workforce. The required training must be provided to each member of the workforce:

1. No later than the date the Practice is required to comply with HIPAA;

2. Within a reasonable period of time after the person joins the covered entity's workforce. Texas requires training within 90 days after the hire date;[2] and

3. Within a reasonable period of time after any material change in the covered entity's privacy policies and procedures that affects the member's functions.

Safeguards to Protect PHI

A covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI. At a minimum, a covered entity must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the Privacy Standards. Certain HIPAA standards apply equally to business associates as they do to covered entities.

HIPAA compliance includes implementing policies and procedures with respect to PHI that comply with the standards, implementation specifications, and other requirements of the Privacy Standards. The policies and procedures must be reasonably designed, taking into account the size and capabilities of the covered entity and the probability and seriousness of the risks to the PHI maintained by the covered entity, to ensure such compliance.

[2] In Texas, if the duties of the employee are affected by a material change in state or federal law on PHI, then the employee must receive training on the effect of the change in law on the employee's duties within 1 year of the change in law taking effect. Tex. Health & Safety Code 181.101.

A covered entity must make changes to its policies and procedures as necessary and appropriate to comply with changes in the Privacy Standards. When a covered entity changes a privacy practice that is stated in its Notice of Privacy Practices and makes corresponding changes to its policies and procedures, it may make the changes effective for PHI that it created or received prior to the effective date of the notice revision under certain circumstances. The changes may cover all PHI if the covered entity has included in its Notice of Privacy Practices a statement reserving its right to make such a change in its privacy practices. A covered entity may make any other changes to its privacy policies and procedures at any time, provided that the changes are documented and implemented in accordance with the Privacy Standards.

Whenever there is a change in law that necessitates a change to the covered entity's privacy policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of its Notice of Privacy Practices, the covered entity must promptly make the appropriate revisions to the notice.

A covered entity must maintain its privacy policies and procedures and other documentation required by HIPAA in either written or electronic form. Documentation of these policies and procedures or other documentation may be kept in either electronic or written form and must be maintained for six years from the date of its creation or the date when it last was in effect, whichever is later.

Complaint Process

In addition, a covered entity must provide a process for individuals to make complaints concerning the covered entity's compliance with HIPAA. All complaints, and the disposition of each, must be documented. A covered entity has a duty to mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of PHI in violation of its policies and procedures or HIPAA. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with its privacy policies and procedures or the requirements of HIPAA. If a covered entity sanctions an employee for violations of its HIPAA policy and procedures, it must document the sanctions.

A covered entity is prohibited from intimidating or retaliatory acts. A covered entity may not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by, HIPAA, including the filing of a complaint with the Secretary of the Department of Health and Human Services (HHS) pursuant to the Privacy Standards.

INDIVIDUAL RIGHTS UNDER HIPAA

The Privacy Standards give individuals the following rights in relation to their PHI.

1. The right to receive written notice of a covered entity's information practices and the individual's rights;

2. The right to access and obtain a copy of the individual's own PHI;

3. The right to obtain an accounting of how the individual's PHI has been disclosed;

4. The right to request a correction and/or amendment of the individual's PHI;

5. The right to request additional restrictions on the use and disclosure of the individual's PHI by the covered entity;

6. The right to request confidential communication of PHI; and

7. The right to file a complaint if the individual believes his or her rights have been violated.

Right to Receive Written Notice

HIPAA provides individuals with the right, unless specifically excepted by the statute, to be notified of the types of uses and disclosures of PHI that may be made by a covered entity. HIPAA also gives individuals the right to be notified of the covered entity's legal duties and the individual's rights in respect to PHI.

Section 164.520(a) of the Privacy Standards provides that a patient has a right to receive written notice of the uses and disclosures (Notice of Privacy Practices) of PHI that might be made by the covered entity and the covered entity's legal duties with respect to PHI maintained by it. The required Notice of Privacy Practices must be a separate document. The Notice of Privacy Practices should be provided to a patient prior to the patient receiving services. A covered entity is required to document its compliance with the Notice of Privacy Practices requirements.

The Notice of Privacy Practices required by Section 164.520(a) must be written in plain language and include:

1. The following statement, as a header or otherwise prominently displayed: "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."

2. Information regarding use and disclosures of PHI:

A. A description including at least one example of the types of uses and disclosures that the covered entity is permitted to make for each of the following: treatment, payment and health care operations;

B. A description of each of the other purposes for which the covered entity is permitted or required to use or disclose PHI without the authorization of the individual;

C. Any limits on the use or disclosure of PHI that is covered by other applicable and more stringent laws;

D. A description of the types of uses and disclosures that require a written authorization with a statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization.

The required descriptions must be in sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by HIPAA and other applicable law.

3. If the covered entity intends to engage in fundraising communications, a statement that the covered entity may contact the individual to raise funds and that the individual has a right to opt out of receiving such communications.

4. If the covered entity receives substance use disorder treatment records, then (i) such records will not be used or disclosed in any proceeding without a court order or written consent by the individual, and (ii) if the covered entity intends to use or disclose such records for fundraising, the individual must first be provided with a clear and conspicuous opportunity to elect not to receive any fundraising communications.

5. Information regarding individual rights with respect to PHI and a brief description of how the individual may exercise these rights. These rights include:

A. The right to request restrictions on certain uses and disclosures of PHI, including a statement that the covered entity is not required to agree to a requested restriction except in the case of certain disclosures of PHI to a health plan where the individual or another person pays out of pocket in full for the health care item or service;

B. The right to receive confidential communication of PHI as provided by HIPAA;

C. The right to inspect and copy PHI;

D. The right to amend PHI;

E. The right to receive an accounting of disclosures of PHI; and

F. The right to receive a paper copy of the Notice of Privacy Practices.

6. Information related to the covered entity's duties including:

A. A statement that the covered entity is required by law to maintain the privacy of PHI, to provide individuals with notice of its legal duties and privacy practices with respect to PHI, and to notify affected individuals following a breach of unsecured PHI;

B. A statement that the covered entity is required to abide by the terms of its Notice of Privacy Practices currently in effect; and

C. If the covered entity wishes to apply changes to its Notice of Privacy Practices to PHI obtained prior to the effective date of the change, a statement that the covered entity reserves the right to change the terms of its Notice of Privacy Practices and to make the changes applicable to all PHI maintained by the covered entity. The statement must also describe how the covered entity will provide individuals with a copy of the revised Notice of Privacy Practices.

7. A statement that individuals may complain to the covered entity and to the Secretary of the HHS if they believe their privacy has been violated;

8. A brief description of how the individual may file a complaint with the covered entity and to the Secretary of HHS if he or she believes that his or her privacy rights have been violated, a brief description of how an individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint;

9. The name, or title, and telephone number of a person or office to contact for further information; and

10. The effective date of the Notice of Privacy Practices.

A covered health care provider that has a direct treatment relationship with an individual must:

1. Provide the notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or, in an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation;

2. Have the notice available at the physical service delivery site for individuals to request to take with them;

3. Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

4. Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of the Privacy Standards.

If a covered entity maintains a website that posts information about its customer services or the benefits provided by the covered entity, it must prominently display its Notice of Privacy Practices on its website and make the notice available electronically through its website. A covered entity may provide the Notice of Privacy Practices electronically if an individual agrees to an electronic notice and such agreement has not been withdrawn. In the event that the covered entity determines that an email transmission has failed, a paper copy of the notice must be provided. If the first service provided to an individual is provided electronically, then the covered entity must provide the electronic notice automatically and contemporaneously in response to the individual's first request for care. An individual who receives the Notice of Privacy Practices electronically retains the right to request a paper copy from the covered entity.

A covered entity must make a good faith effort to obtain a signed Acknowledgment documenting receipt of the Notice of Privacy Practices by the individual. All efforts and reason(s) why the Acknowledgment was not obtained must be documented. The inability to obtain an Acknowledgment does not prohibit the use of PHI for purposes of treatment, payment and health care operations. A sample Acknowledgment is provided as Exhibit A3.

Additionally, Section 1557 of the Patient Protection and Affordable Care Act (ACA) prohibits discrimination on the basis of race, color, national origin, sex, age, or disability in health programs or activities that receive Federal financial assistance or are administered by an Executive agency or any entity established under Title I of the ACA. Pursuant to Section 1557 and its implementing regulation, covered health care providers are required to post, in their significant publications and communications, nondiscrimination notices in English and taglines advising the reader of the availability of free language assistance services in at least the top 15 languages spoken by individuals with limited English proficiency (LEP) in the state(s) in which the covered entities operate. HHS has published guidance indicating that a covered entity's Notice of Privacy Practices constitutes a communication that is "significant" for purposes of Section 1557 and its regulations. As such, a covered entity's Notice of Privacy Practices must include the applicable non-discrimination notice language as well as the appropriate 15 taglines. A sample notice and translated taglines are available on HHS' website.

In order to comply with Section 164.520 a covered entity must:

1. Develop a Notice of Privacy Practices that includes all the elements required by the Privacy Standards. A sample Notice of Privacy Practices is attached as Exhibit A1.

2. Develop policies and procedures to:

   - Ensure that each individual is provided with a copy of its Notice of Privacy Practices;
   - Document the provision of the Notice of Privacy Practices to individuals;
   - If the covered entity maintains a website, ensure that its Notice of Privacy Practices is posted on the website and available electronically;
   - Retain copies of the notices that it issues; and
   - Ensure that any changes to the covered entity's Notice of Privacy Practices and its practices comply with the Privacy Standards.

A sample policy and procedure is attached as Exhibit A2.

Access

Upon a request for access from an individual, a covered entity must provide the individual access to and a copy of the individual's PHI, except for psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding, in order for the individual to inspect and view the PHI the covered entity maintains about the individual. A covered entity may require individuals to make requests for access in writing provided that the covered entity informs individuals of the requirement.

Once a request for access is received by a covered entity, the covered entity must act on a request for access no later than 30 days[3] after receipt of the request as follows:

1. If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested in accordance with the Privacy Standards; or

2. If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial in accordance with the Privacy Standards.

If a covered entity is unable to respond as required by the Privacy Standards within the times specified, the covered entity may have an additional 30 days to respond, provided the covered entity, within the time limit set by the Privacy Standards, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request. The covered entity may have only one such extension of time for action on a request for access.

A summary or explanation of the PHI may be provided by the covered entity if:

---

[3] State statutes may require a provider to allow a patient access to his/her medical records in less than thirty days. In such cases, the state statute will allow greater protection to the patient, and the covered entity must comply with the state statutory requirements. In Texas, dental records must be provided to a patient within 30 days of receiving the request. 22 TAC § 108.8.

1. The individual agrees in advance to such a summary or explanation; and

2. The individual agrees in advance to any fees imposed by the covered entity for such summary or explanation.

If the individual requests a copy of the PHI, or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of copying, including the cost of supplies for and labor of copying, the PHI requested by the individual.[4] A covered entity may also charge for postage when the individual has requested that the copy, summary or explanation be mailed. Finally, a covered entity may charge for preparing an explanation or summary of the PHI if agreed to by the individual in advance.[5]

If the covered entity grants a request for access, in whole or in part, to PHI, the covered entity must

1. Provide the access requested by the individual in a timely manner, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request;

2. Provide access to the PHI in the form and format requested by the individual, if it is readily producible in such form and format or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual; and

3. If the requested PHI is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with 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 the covered entity and the individual.

If an individual requests the covered entity to transmit the copy of PHI to another person designated by the individual, the covered entity must provide the copy to the person so designated. Such a request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI.

There are some situations where an individual may be denied a right to access. In most cases, if a covered entity denies an individual access to the individual's PHI, the individual must be given the right to have the denial reviewed. An individual has the right to a review of the denial if access to PHI is denied in the following circumstances:

---

[4] Texas law allows a dentist to charge up to $25 for the first 20 pages and $0.15 per page thereafter. There are other limits for rediographs. See, 22 TAC §108.8.

[5] Fees related to the provision of medical records are often governed by state statute. In the event a state statute provides a more restrictive fee schedule, the state statute will apply.

1. A licensed health care professional has determined, in the exercise of professional judgment, that granting the requested access is reasonably likely to endanger the life or physical safety of the individual or another person;

2. The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that granting the access requested is reasonably likely to cause substantial harm to such other person; or

3. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of such access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

If an individual is denied access based on one of the reasons set forth above, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny access to the records. The covered entity must promptly refer a request for review to such designated reviewing official. The reviewing official must make a determination in a reasonable amount of time. The standards do not define a reasonable amount of time. The covered entity is bound by the decision of the reviewing official, must promptly provide written notice to the individual of the decision, and must provide or deny access in accordance with the determination of the reviewing official.

A covered entity may deny an individual access without the opportunity for review only in the following circumstances:

1. The PHI is exempt from the right of access because:

   A. The PHI meets the definition of psychotherapy notes;

   B. The PHI was compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

2. The covered entity is a correctional institution or the provider is acting under the direction of a correctional institution and obtaining a copy would jeopardize:

   A. The health, safety, security, custody or rehabilitation of the individual or of other inmates; or

   B. The safety of any officer, employee or other person at the correctional institution or an individual responsible for the transportation of the inmate.

3. An individual's access to PHI created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the

denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research;

4. An individual's access to PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied if the access could be denied under terms of the Privacy Act; and

5. An individual's access may be denied if the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

If a covered entity has a right to deny access to PHI and, in fact, denies access to PHI, the covered entity must comply with the following requirements:

1. The covered entity must, to the extent possible, give the individual access to any other PHI requested after excluding the PHI as to which the covered entity has a ground to deny access;

2. The covered entity must provide a timely, written denial to the individual in accordance with the Privacy Standards. The denial must be in plain language and contain:

   A. The basis for the denial; and

   B. If applicable, a statement of the individual's review rights under the Privacy Standards, including a description of how the individual may exercise such review rights; and

   C. A description of how the individual may complain to the covered entity or to the Secretary of HHS. The description must include the name or title and telephone number of the contact person or office designated to accept complaints.

If the covered entity does not maintain the PHI that is the subject of the individual's request for access, and the covered entity knows where the requested PHI is maintained, the covered entity must inform the individual where the covered entity believes the PHI is maintained.

In order to comply with Section 164.524, a covered entity must develop policies and procedures for:

- Documenting the designated record set that are subject to access by individuals and the title or persons or offices responsible for receiving and processing requests for access by individuals;
- Receipt of a request for access;
- Responding to a request for access;

- Denying a request for access;
- Reviewing a denial of a request for access;
- Timely replying to a request for access; and
- Documenting all actions taken as a result of the request.

A sample policy and procedure is attached as Exhibit B.

Accounting of Disclosures

Section 164.528(a) of the Privacy Standards gives an individual the right to receive an accounting for disclosures of PHI made by a covered entity for the six years[6] prior to the date on which the accounting is requested. Under HITECH, a covered entity that uses or maintains electronic health records (EHRs) must account for disclosures of an individual's EHR for purposes of treatment, payment and health care operations for a period of three years prior to the individual's request.[7] The six-year accounting period under HIPAA remains intact for all other disclosures.

The accounting is not required to include disclosures:

1. For purposes of treatment, payment and health care operations, if the covered entity does not use or maintain EHRs;

2. To individuals of their own PHI in accordance with an individual's right to access;

3. For the facility's directory or to persons involved in the individual's care or other notification purposes as provided by the Privacy Standards;

4. For national security or intelligence purposes as provided in accordance with the Privacy Standards;

5. To correctional institutions or law enforcement officials in accordance with the Privacy Standards;

6. That occurred prior to the compliance date for the covered entity;

7. That were made in accordance with a valid authorization;

8. As part of a limited data set in accordance with the Privacy Standards; and

9. Incident to a use or disclosure otherwise permitted or required by the Privacy Standards.

---

[6] However, an individual may request an accounting for a period of less than six years.

[7] The HITECH Act required the Secretary of HHS to adopt implementing regulations, which have not been finalized. As of this writing, the current 45 CFR 164.528(a) does not require an accounting of disclosure for treatment, payment, or health care operations when PHI is maintained in an EHR.

If requested, a covered entity must provide the individual with a written accounting that meets the following requirements:

1. The accounting must include disclosures of PHI (other than PHI in the excepted categories listed above) that occurred during the six years (or a shorter time period if requested by the individual) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

2. For each disclosure the accounting must include:

   A. The date of the disclosure;

   B. The name of the entity or person who received the PHI and, if known, the address of such entity or person;

   C. A brief description of the PHI disclosed;

   D. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

If during the period covered by the accounting, the covered entity has made multiple disclosures of PHI to the same person or entity for a single purpose or pursuant to a single authorization, the accounting, with respect to such multiple disclosures must provide:

1. The information required by the Privacy Standards of this section for the first disclosure during the accounting period;

2. The frequency, periodicity or number of the disclosures made during the accounting period; and

3. The date of the last such disclosure during the accounting period.

When an individual requests an accounting from a covered entity, the covered entity must act on the individual's request for an accounting no later than 60 days after receipt of such a request. If the covered entity is unable to provide an accounting within 60 days as required by the Privacy Standards, the covered entity may have one 30-day extension if, within the initial 60-day period, the covered entity provides the individual with a written statement of the reasons for the delay and the date by which it will provide the accounting.

A covered entity must provide the first accounting to an individual in any 12-month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, provided that the covered entity informs the individual, in advance, of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

If the agency's or official's statement is made orally, the covered entity must:

1. Document the statement, including the identity of the agency or official making the statement;

2. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

3. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to 45 CFR 164.528(a)(2)(i) is submitted during that time.

Compliance with Section 164.528 requires covered entities to establish policies and procedures to:

- track the disclosure of PHI;
- determine whether or not a particular disclosure must be included in an accounting;
- document all requests for an accounting and the final disposition of all such requests; and
- provide an accounting to an individual in a timely manner.

Sample policies and procedures are attached as Exhibits C1 and C2.

Correction and/or Amendment

Section 164.526(a) of the Privacy Standards gives an individual the right to request that a covered entity amend PHI maintained by the covered entity. A covered entity is not required to amend PHI and may deny an individual's request for amendment if the covered entity determines that:

1. The PHI was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

2. The PHI is not part of the designated record set maintained by the covered entity;

3. The requested amendment concerns information that would not be subject to a right to inspect and copy pursuant to the Privacy Standards; or

4. The PHI is accurate and complete.

A covered entity may require individuals to request an amendment in writing, and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements. A covered entity must act upon a request for amendment no later than 60 days after receipt of such a request and may have one 30-day extension if, within the initial 60-day period, the covered entity provides the individual with a written statement of the reasons for the delay and the date by which it will complete its action.

If a covered entity agrees to amend its records, the covered entity must make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment. A covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of the persons with whom the amendment needs to be shared, and agreement that the covered entity may notify those persons.

The covered entity must make reasonable efforts to provide the amendment within a reasonable time to persons identified by the individual and persons, including business associates, that the covered entity knows have the PHI that is the subject of the amendment and that may have relied, or it is foreseeable could rely, on such information to the detriment of the individual.

If a covered entity is informed by another covered entity of an amendment to an individual's PHI, the covered entity must amend the PHI it maintains.

If the covered entity denies the requested amendment, the covered entity must provide the individual with a timely, written denial. The denial must use plain language and contain:

1. The basis for the denial;

2. A statement that the individual has a right to submit a written statement disagreeing with the denial (Statement of Disagreement) and how the individual may file such a statement;

3. A statement that, if the individual does not submit a Statement of Disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment;

4. A description of how the individual may complain to the covered entity. The description must include the name or title, and telephone number of the contact person or office designated to accept complaints; and

5. A description of how the individual may complain to the covered entity or to the Secretary of HHS, including contact information.

The covered entity must permit the individual to submit to the covered entity a written Statement of Disagreement disagreeing with the denial of all or part of a requested amendment and the basis

of such disagreement. The covered entity may reasonably limit the length of a Statement of Disagreement. The covered entity may prepare a written Rebuttal to the individual's Statement of Disagreement. If a Rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the Statement of Disagreement.

The covered entity must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's Statement of Disagreement, if any, and the covered entity's Rebuttal, if any, to the designated record set.

If a Statement of Disagreement has been submitted by the individual, the covered entity must include the Statement of Disagreement or an accurate summary of the Statement of Disagreement with any subsequent disclosure of the PHI to which the Statement of Disagreement relates.

If the individual has not submitted a written Statement of Disagreement, the covered entity must include the individual's request for amendment and its denial or an accurate summary of the request with any subsequent disclosure of the PHI only if the individual has requested such action in accordance the Privacy Standards.

A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments in accordance with the Privacy Standards.

To comply with Section 164.526, a covered entity must establish policies and procedures to be followed when the covered entity receives a request for amendment, for determining whether to amend or deny a request for amendment, for amending PHI as requested, for processing amendments received from other health care providers, and for denial of a request for amendment including how to process Statements of Disagreement and Rebuttals. A sample policy and procedure is attached as Exhibit D.

Restriction of Use

Section 164.522(a)(1) of the Privacy Standards gives an individual the right to request restrictions of uses and disclosure of PHI. Generally, HIPAA does not require a covered entity to agree to additional restrictions. However, HIPAA requires a covered entity to agree to a requested restriction if:

1. The disclosure is to a health plan for purposes of carrying out payment or health care operations and not for carrying out treatment;

2. The disclosure is not otherwise required by law; and

3. The PHI pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket in full.

A covered entity that agrees to a restriction may not use or disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency

treatment and the restricted PHI is needed to provide the emergency treatment, the covered entity may use the restricted PHI, or may disclose such information to a health care provider, to provide such treatment to the individual. If restricted PHI is disclosed to a health care provider for emergency treatment, the covered entity must request that such health care provider not further use or disclose the information.

If a covered entity agrees to an individual's request for restriction, the restriction must be documented. This includes, if applicable, documentation of the termination of any agreement to restrict the release of PHI. An agreement to restrict the disclosure of PHI may be terminated:

1. If the individual requests or agrees to the termination in writing;

2. If the individual agrees orally and the oral agreement is documented; or

3. If the covered entity informs the individual that it is terminating its agreement to a restriction.

If a covered entity terminates its agreement, the termination is only effective with respect to PHI obtained after it has notified the individual.

Confidential Communications

Section 164.522(b)(1) of the Privacy Standards allows individuals the right to request to receive communications of PHI by alternative means or at alternative locations. A covered entity may request that the individual make the request in writing.

A covered entity must accommodate all reasonable requests for confidential communications. However, a covered entity may condition the provision of a reasonable accommodation on the following:

1. When appropriate, information as to how payment, if any, will be handled; and

2. Specification of an alternative address or other method of contact.

A covered health care provider may not request an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

Compliance with Section 164.522 requires a covered entity to establish policies and procedures for an individual to request additional restrictions, for allowing or denying a request for additional restrictions, for documenting any agreed-to restrictions, for ensuring compliance with any agreed-to restrictions, and for terminating a restriction. A sample policy and procedure is attached as Exhibit E.

AUTHORIZATIONS

The Privacy Standards lists certain kinds of uses and disclosures of PHI that do not require the individual's permission. Before making any use or disclosure of PHI that is not included in that list, a covered entity must obtain a written authorization from the individual. An authorization gives a covered entity permission to use specific PHI for limited purposes or to disclose PHI to a third party specified by the individual. An authorization only covers the uses and disclosures and only the PHI stipulated in the authorization. An authorization must have an expiration date or expiration event. Treatment may not be conditioned on the individual providing an authorization except in limited circumstances.

The basic requirements of authorization are that a valid authorization must:

1. Be in plain language;

2. Provide a specific and meaningful description of the information to be used or disclosed;

3. Specifically name the person or class of persons to whom the covered entity may disclose;

4. Name or specifically identify the person or class of persons who may make the disclosure;

5. State that the individual has the right to revoke the authorization in writing, and either the exceptions to the right to revoke and a description if how the individual may revoke the authorization or, if the information is contained in a Notice of Privacy Practices, a reference to the document;

6. Provide an expiration date or expiration event;

7. Be signed and dated;

8. If signed by a personal representative, give a description of the personal representative's authority to act on behalf of the individual;

9. Inform the individual of the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by the Privacy Standards;

10. Describe each purpose of the requested use or disclosure; and

11. State either

    A. The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization

when the prohibition on conditioning of authorizations as set forth in the Privacy Standards applies; or

B. The consequences to the individual of a refusal to sign the authorization when, in accordance with the Privacy Standards, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

A valid authorization may contain information in addition to the basic elements set forth above, provided that such additional elements or information are not inconsistent with the required elements. A covered entity must document, if applicable, its compliance with the requirement to have an authorization prior to releasing information.

An authorization is not valid if the document has any of the following defects:

1. The authorization lacks any of the basic elements as set forth above;

2. The expiration date has passed or the expiration event is known by the covered entity to have occurred;

3. The authorization has not been filled out completely, with respect to the basic elements, as set forth above;

4. The authorization is known by the covered entity to have been revoked;

5. Any material information in the authorization is known by the covered entity to be false; or

6. The authorization was combined with another document in violation of the Privacy Standards.

An individual may revoke an authorization provided under this section at any time, provided the revocation is in writing, except to the extent that the covered entity has taken action in reliance of the authorization.

A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan or eligibility for benefits on the provision of an authorization, except:

1. A health care provider may condition the provision of research-related treatment on provision of an authorization for research; or

2. A covered entity may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.

A covered entity must provide the individual with a copy of the signed authorization.

In order to comply with the authorization requirements of Section 164.508 of the Privacy Standards a covered entity must:

1. Develop the appropriate authorization forms which include the required elements. A sample Authorization Form is attached as Exhibit F1.

2. Establish policies and procedures for:

   - documenting and retaining authorizations received by the covered entity;
   - handling authorizations and requests for PHI from outside entities;
   - ensuring that an individual is given a copy of any authorization obtained by the covered entity; and
   - prohibiting the release of PHI to external entities without obtaining the proper authorization.

A sample policy and procedure is attached as Exhibit F2.

USES AND DISCLOSURES OF PHI

Uses and Disclosures in General

A covered entity or business associate may not use or disclose PHI, except as permitted or required by HIPAA and its implementing regulations. The applicable restrictions and requirements for using or disclosing PHI depends on the nature of the use or disclosure. A covered entity must comply with the requirements of the Privacy Standards with regard to the PHI of a deceased individual for a period of 50 years following the date of death.

Disclosures for Treatment, Payment or Health Care Operation Purposes

A covered entity may:

1. Use or disclose PHI for its own treatment, payment, or health care operations;

2. Disclose PHI for treatment activities of a health care provider;

3. Disclose PHI to another covered entity or a health care provider for the payment activities of the entity that receives the information; and

4. Disclose PHI to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

    A. For certain health care operations, specifically identified in § 164.506(c)(4)(ii); or

    B. For the purpose of health care fraud and abuse detection or compliance.

Disclosures of PHI without an Authorization or Opportunity to Agree or Object

A covered entity may release PHI without an authorization, and without giving the individual an opportunity to object, in the following situations:

1. Use or disclosure required by law including:

    A. Disclosure regarding victims of abuse, neglect or domestic violence;

    B. Disclosure for judicial and administrative proceedings; and

    C. Disclosure for law enforcement;

2. Use or disclosure for public health activities;

3. Use or disclosure for health oversight activities;

4. Use or disclosure about decedents;

5. Use or disclosure for cadaveric organs, eye or tissue donations;

6. Use or disclosure for research purposes;

7. Use or disclosure to avert serious threats to health or safety;

8. Use or disclosure for specialized government functions; and

9. Disclosure for Worker's Compensation.

Disclosures Allowed by the Law

As stated above, a covered entity may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with, and is limited to, the relevant requirements of such law. The requirements for such use or disclosure are found in the sections of the Privacy Standards on:

1. Disclosures about victims of abuse, neglect or domestic violence;

2. Disclosures for judicial or administrative proceedings; and

3. Disclosures for law enforcement purposes.

Disclosures About Victims of Abuse, Neglect or Domestic Violence

Pursuant to Section 164.512(c), a covered entity may disclose PHI about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence:

1. To the extent the disclosure is required by law and the disclosure complies with, and is limited to, the relevant requirements of such law;

2. If the individual agrees to the disclosure; or

3. To the extent the disclosure is expressly authorized by statute or regulation, and:

    A. The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

B. If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A covered entity that makes such a disclosure must promptly inform the individual that such a report has been or will be made unless:

1. The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

2. The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

Disclosures for Judicial and Administrative Proceedings

Pursuant to Section 164.512(e), a covered entity may disclose PHI in the course of any judicial or administrative proceeding:

1. In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the PHI expressly authorized by such order; or

2. In response to a subpoena, discovery request or other lawful process that is not accompanied by an order of a court or administrative tribunal if:

   A. The covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the PHI has been given notice of the request; or

   B. The covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of HIPAA.

3. For purposes of HIPAA, a covered entity receives satisfactory assurances from a party seeking PHI if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

   A. The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

B. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and

C. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

i. No objections were filed; or

ii. All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

D. The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

E. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

4. A *qualified protective order* means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

A. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and

B. Requires the return to the covered entity or destruction of PHI (including all copies made) at the end of the litigation or proceeding.

Disclosures for Law Enforcement Purposes

Section 164.512(f) of the Privacy Standards provides that a covered entity may disclose PHI for law enforcement purposes to a law enforcement official:

1. As required by law including laws that require the reporting of certain types of wounds or other physical injuries; or

2. In compliance with, and as limited by, the relevant requirements of:

A. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

B. A grand jury subpoena; or

C. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand or similar process authorized under law, provided that:

i. The information sought is relevant and material to a legitimate law enforcement inquiry;

ii. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

iii. De-identified information[8] could not reasonably be used.

In addition, covered entities are permitted to disclose certain information to law enforcement officials for the following purposes:

1. Response to request for information for identification and location purposes, if limited to:

   A. Name and address;

   B. Date and place of birth;

   C. Social security number;

   D. ABO blood type and rh factor;

   E. Type of injury;

   F. Date and time of treatment;

   G. Date and time of death; if applicable; and

   H. A description of distinguishing physical characteristics.

2. Response to request for information about an individual who is or is suspected to be a victim of a crime if:

   A. The individual agrees to the disclosure; or

   B. The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

      i. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other

[8] De-identified information is discussed below in the section entitled "De-Identified Information."

than the victim has occurred, and such information is not intended to be used against the victim;

ii. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

iii. The disclosure is in the best interest of the individual as determined by the covered entity, in the exercise of professional judgment.

3. Provide information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

Disclosures for Health Oversight Activities

Section 164.512(d) of the Privacy Standards provides a covered entity may disclose PHI 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:

1. The health care system;

2. Government benefit programs for which health information is relevant to beneficiary eligibility;

3. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

4. Entities subject to civil rights laws for which health information is necessary for determining compliance.

Health oversight activities do not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

1. The receipt of health care;

2. A claim for public benefits related to health; or

3. Qualification for, or receipt of, public benefits or services when an individual's health is integral to the claim for public benefits or services.

Notwithstanding this exception, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not

related to health care, the joint activity or investigation is considered a health oversight activity for purposes of HIPAA.

Disclosures for Public Health Activities

A covered entity may disclose PHI to the following:

1. A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

2. A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect; or

3. A person subject to the jurisdiction of the Food and Drug Administration:

    A. To report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations if the disclosure is made to the person required or directed to report such information to the FDA;

    B. To track products if the disclosure is made to a person required or directed by the FDA to track the product;

    C. To enable product recalls, repairs or replacement (including locating and notifying individuals who have received products of product recalls, withdrawals or other problems); or

    D. To conduct post marketing surveillance to comply with FDA requirements or at the direction of the FDA;

4. A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

5. An employer, about an individual who is a member of the employer's workforce, if:

A. The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer:

i. To conduct an evaluation relating to medical surveillance of the workplace; or

ii. To evaluate whether the individual has a work-related illness or injury;

B. The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

C. The employer needs such findings in order to comply with regulations of the Occupational Safety and Health Administration or the Mine Safety and Health Administration, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance;

D. The covered entity provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

i By giving a copy of the notice to the individual at the time the health care is provided; or

ii. If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

Uses or Disclosures Requiring an Opportunity to Agree or Object

A covered entity may use or disclose PHI in the following ways, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure:

1. Disclosure to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care;

2. Use or disclosure PHI to notify, or assist in the notification of a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.

Communications for the two purposes described above must be made in accordance with the following:

1. If the individual is present for, or otherwise available prior to, a permitted use or disclosure and has the capacity to make health care decisions, the covered entity may use or disclose the PHI if it:

   A. Obtains the individual's agreement;

   B. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

   C. Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

2. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

3. If the individual is deceased, a covered entity may disclose to a family member, or other identified persons who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

4. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.

Compliance with the standards related to disclosures otherwise allowed by law requires covered entities to establish policies and procedures for:

- determining whether a disclosure without authorization for purposes other than those otherwise allowed by law; and

- documenting the disclosure of PHI for Public Health Activities and including such disclosures on an accounting provided to an individual.

A sample policy and procedure is attached as Exhibit G.

Disclosure for Fundraising

Subject to certain requirements, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following PHI for the purpose of raising funds for its own benefit, without first obtaining an authorization from the individual:

1. Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

2. Dates of health care provided to an individual;

3. Department of service information;

4. Treating physician;

5. Outcome information; and

6. Health insurance status.

With each fundraising communication, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

With regards to its fundraising activities, a covered entity may not:

1. Condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications;

2. Use or disclose PHI for fundraising purposes unless a statement to that effect is included in the covered entity's Notice of Privacy Practices; or

3. Make fundraising communications to an individual if the individual has elected not to receive such communications. However, a covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

DISCLOSURE OF PHI TO A PERSONAL REPRESENTATIVE

Section 164.502(g) governs the release of PHI to personal representatives. As a general rule, personal representatives stand in the shoes of the individual and may consent or authorize the use and disclosure of PHI.

A person can be considered a personal representative of an adult or emancipated minor if under applicable law a person has the authority to act on behalf of the individual in making decisions related to health care. In the case of a minor that is not emancipated, a parent, guardian or other person acting in loco parentis that has authority under applicable law to act on behalf of the minor in making decisions related to health care is considered a personal representative. However, the minor that is not emancipated has the authority to act as an individual with respect to PHI pertaining to a health service if:

1. The minor assents to health care service, no other consent is required by law regardless of whether or not the consent of another has been obtained, and the minor has not requested that such person be treated as a personal representative;

2. The minor may lawfully obtain such health care service without the consent of another, and the minor, a court or another person authorized by law has consented to such health care service; or

3. The parent, guardian or other person acting in loco parentis agrees to an agreement of confidentiality between the covered entity and the minor.

The personal representative of an individual has the same rights and responsibilities as the individual. However, a covered entity may elect not to disclose PHI to a personal representative if the covered entity has a reasonable belief that:

1. The individual may be subject to abuse or neglect; or

2. Treating the person as the personal representative might endanger the individual and it is not in the best interest of the individual to treat the person as a personal representative.

Compliance with Section 164.502(g) requires a covered entity to:

1. Be familiar with state law regarding personal representatives; and

2. Establish policies and procedures for the release of information to a personal representative. A sample policy and procedure is attached as Exhibit H.

SALE OF EHR OR PHI

Under HIPAA, a covered entity or business associate may not sell PHI without a valid authorization. The authorization must state that the disclosure will result in remuneration to the covered entity.

A "sale of PHI" is defined as "a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information." However, the sale of PHI does not include a disclosure of PHI:

1. For public health purposes;

2. For research purposes so long as the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;

3. For treatment and payment disclosures;

4. For the sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity, and related due diligence;

5. To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

6. To the individual upon appropriate request;

7. As required by law; and

8. For any other purpose permitted by and in accordance with the Privacy Rule where the covered entity receives only a cost-based fee to cover the cost to prepare and transmit the PHI or a fee otherwise expressly permitted by other law.

The Office for Civil Rights ("OCR") specifically stated within its preamble comments that the prohibition against the sale of protected health information applies to the receipt of nonfinancial as well as financial benefits. Therefore, a covered entity or business associate may not disclose PHI in exchange for in-kind benefits, unless the disclosure meets one of the exceptions listed above.

As noted within the sale of PHI exceptions above, the final rule authorizes a covered entity or business associate to receive remuneration in the form of reasonable, cost-based fees to cover the

cost of preparing and transmitting PHI for specific disclosures. Within its preamble comments, the OCR clarified that reasonable cost-based fees may include the following:

1. Both direct and indirect costs, including labor, materials, and supplies for generating, storing, retrieving, and transmitting PHI;

2. Labor and supplies to ensure the PHI is disclosed in a permissible manner;

3. Related capital and overhead costs.

However, the OCR specifically disallows "fees charged to incur a profit from the disclosure of protected health information," which would prohibit a covered entity or business associate from achieving a profit margin based on remuneration associated with preparing and transmitting PHI.

DE-IDENTIFIED INFORMATION

Health information that does not identify an individual and, with respect to which there is no reasonable basis to believe that the information can be used to identify an individual, is not individually identifiable health information. A covered entity may determine that health information is not individually identifiable, and therefore is not PHI, only if:

1. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

    A. Applying such principles and methods determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

    B. Documents the methods and results of the analysis that justify such determination; or

2. The following identifiers of the individual or of relatives, employers or household members of the individual, are removed:

    A. Names;

    B. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people. If the geographic unit formed by combining all zip codes with the same three initial digits contains 20,000 or fewer people, the initial three digits of the must be changed to 000;

    C. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

    D. Telephone numbers;

    E. Fax numbers;

    F. Electronic mail addresses;

    G. Social security numbers;

H. Medical record numbers;

I. Health plan beneficiary numbers;

J. Account numbers;

K. Certificate/license numbers;

L. Vehicle identifiers and serial numbers, including license plate numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers;

P. Biometric identifiers including finger and voice prints;

Q. Full face photographic images and any comparable images; and

R. Any other unique identifying number, characteristic or code.

Even with all of these identifiers removed, health information is not considered de-identified if the covered entity has actual knowledge that the information could be used, alone or in combination with other information, to identify an individual who is a subject of the information.

A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity provided that:

1. The code or other means of record identification is not derived from, or related to, information about the individual and is not otherwise capable of being translated so as to identify the individual; and

2. The covered entity does not use or disclose the code or other means of record identification for any other purpose and does not disclose the mechanism for re-identification.

A covered entity must have in place a policy and procedure to prevent the release of PHI not otherwise allowed unless the PHI has been de-identified. A sample policy and procedure is attached as Exhibit I.

MINIMUM NECESSARY PHI

Section 164.502(b) of the Privacy Standards requires covered entities to make reasonable efforts to ensure that the minimum necessary amount of PHI is used or disclosed for any reason except for:

1. Disclosures to or requests by a health care provider for treatment;

2. Uses or disclosures made to the individual;

3. Uses or disclosures made pursuant to an authorization;

4. Disclosures made to the Secretary of HHS to investigate a privacy violation;

5. Uses or disclosures that are required by law; and

6. Uses or disclosures that are required for compliance with HIPAA.

A covered entity must limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made when requesting such information from other covered entities. For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made. For all other requests, a covered entity must review the request on an individual basis to determine that the PHI sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.

A covered entity may not use, disclose or request an entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

A covered entity must identify:

1. Those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties; and

2. For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

A covered entity must make reasonable efforts to limit the access of such persons or classes to PHI.

For all other disclosures, a covered entity must:

1. Develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which the disclosure is sought; and

2. Review requests for disclosure on an individual basis in accordance with such criteria.

A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

1. Making disclosures to public officials if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

2. The information is requested by another covered entity;

3. The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

4. Documentation or representations that comply with the applicable requirements of HIPAA have been provided by a person requesting the information for research purposes.

A sample policy and procedure for minimum necessary release of PHI is attached as Exhibit J.

DISCLOSURE OF PHI FOR MARKETING

The HIPAA standards define marketing to mean "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." Marketing does not include communications made for the following purposes:

1. To provide refill reminders or otherwise communication about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication;

2. For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

    A. For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

    B. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about:

        i. The entities participating in a health care provider network or health plan network;

        ii. Replacement of, or enhancements to, a health plan; and

        iii. Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

    C. For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

The definition of marketing is broad and encompasses most marketing activities.

A covered entity may not use or disclose PHI for marketing purposes without an authorization. If the marketing involves financial remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved. The Privacy Standards define the term "financial remuneration" to mean "direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual." In its preamble comments to the final rule, the OCR

noted that financial remuneration includes only payments made in exchange for marketing communications and does not include non-financial benefits, such as in-kind benefits, provided to a covered entity in exchange for communications about a product. Further, the OCR stated that "if the financial remuneration received by the covered entity is for any purpose other than for making the [marketing] communication, then this marketing provision does not apply."

It is important to note that a covered entity is not required to obtain an authorization under Section 164.508(a)(3) of the Privacy Standards when it uses or discloses PHI to make a marketing communication to an individual that:

1. Occurs in a face-to-face encounter with the individual; or

2. Is in the form of a promotional gift of nominal value provided by the covered entity.

A policy and procedure for the release of PHI for marketing purposes is attached as Exhibit K.

BREACH NOTIFICATION

A breach is the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information. The HHS defined "compromises the security or privacy of the protected health information" to mean "poses a significant risk of financial, reputational, or other harm to the individual."

The following are not considered breaches:

1. Unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further impermissible use or disclosure.

2. Inadvertent disclosure of PHI from one person 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, provided there is no further impermissible use or disclosure.

3. 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.

An acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Standards is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the protected health information or to whom the disclosure was made;

3. Whether the protected health information was actually acquired or viewed; and

4. The extent to which the risk to the protected health information has been mitigated.

It is important to note that a risk assessment is required not only for cases of impermissible disclosures to third parties, but also in the case of impermissible use (*e.g.*, use within a covered entity or by a business associate).

A covered entity's or business associate's analysis of the probability that PHI has been compromised must, at a minimum, address each factor above, yet a risk assessment may also include other factors where necessary. According to the OCR's preamble comments, "if an evaluation of the factors above fails to demonstrate that there is a low probability that the PHI has

been compromised, breach notification is required." Although a risk assessment is appropriate for entities that want to demonstrate that notification is not required, because of the reportable breach presumption, an entity is permitted to engage the breach notification procedures and forgo a formal risk assessment.

Covered entities are required to notify individuals when their unsecured PHI has been breached. PHI is considered unsecured unless it has been rendered unusable, unreadable, or indecipherable to unauthorized persons though the use of technology or methodology specified by the Secretary of HHS, such as encryption by processes approved by the National Institute of Standards and Technology (NIST) or equivalent processes, or unless the media on which the PHI is stored or recorded has been (i) destroyed by shredding or otherwise such that the PHI cannot be read or reconstructed, in the case of paper, film, or other hard-copy media, or (ii) cleared, purged, or destroyed consistent with guidelines of the NIST, in the case of electronic media. A business associate of a covered entity must notify the covered entity of a breach, and the notice must include the identification of each individual whose unsecured PHI has been breached.

All notifications of a breach must be made without unreasonable delay, and in no circumstance more than 60 days after the breach is discovered, unless a law enforcement official determines that notification would impede a criminal investigation or damage national security. A breach is considered discovered on the first day such breach is known or, by exercising reasonable diligence, would have been known to the covered entity or business associate, including any employees, officers, or agents. When a breach of unsecured PHI occurs, various methods of notification exist, depending on the number and location of individuals whose PHI has been breached.

Actual Written Notice

Actual written notification must be provided to the individuals affected by the breach, as well as substitute notice to the individual if the individual's contact information is insufficient or out-of-date. Notification must be provided by first class mail at the last known address of the individual or by email. Email is only permissible if the individual has agreed to receive electronic notice and such agreement has not been withdrawn. If the affected individual is deceased, notification must be sent to the individual's next of kin or personal representative if the covered entity knows that the individual is deceased and has the address of the next of kin or personal representative.

Written notifications must be written in plain language and must include the following:

1. A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;

2. A description of the types of unsecured PHI that were involved (i.e. full name, Social Security number, date of birth, etc.);

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what the covered entity is doing to investigate the breach, mitigate harm to individuals, and protect against any further breaches; and

5. Contact procedures for individuals to ask questions and obtain additional information, which must include a toll-free telephone number, an email address, website, or postal address.

If the covered entity does not have sufficient contact information for some or all of the affected individuals or if some notifications are returned as undeliverable, the covered entity must provide substitute notice reasonably calculated to reach the individual as soon as reasonably possible after the covered entity is aware that it does not have sufficient contact information. A covered entity, however, is not required to provide substitute notice for the individual's next of kin or personal representative where there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative. The type of substitute notice depends on the number of individuals the covered entity is unable to contact.

If fewer than ten individuals cannot be reached through actual written notice, the covered entity may provide substitute notice through alternative forms of written communication, telephone, email, a posting of notice on the covered entity's website, or other similar means.

If ten or more individuals cannot be reached via actual written notice, the covered entity must provide substitute notice through either a conspicuous posting on the covered entity's web site home page for 90 days or conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals likely reside. Additionally, the covered entity must set up a toll-free telephone number, active for at least 90 days, where individuals can determine if his or her PHI was included in the breach. This toll-free number must be included in the substitute notice.

In cases where the covered entity determines there is imminent danger that the unsecured PHI will be misused, notice by telephone or other means may be made, in addition to the written notice required.

Notification to the Media

If 500 or more individuals in any one state or jurisdiction are affected by a breach of unsecured PHI, in addition to providing written notice as described above, a covered entity must notify prominent media outlets serving the state or jurisdiction without unreasonable delay and in no case more than 60 days after the breach was or reasonably could have been discovered. The notification to the media must include the same information as required in the actual written notice.

Notification to the Secretary

If more than 500 individuals are affected by a breach of unsecured PHI, the covered entity must notify the Secretary of the breach without unreasonable delay but in no case more than 60 days after the breach is discovered (i.e., contemporaneously with notice to the individuals). The notification to the Secretary must be provided if more than 500 individuals are affected, regardless of whether the individuals are residents of a particular state or jurisdiction (unlike the notification

to the media standard). Information regarding the manner of reporting breaches may be found on the HHS website. The HHS website will maintain a list of covered entities that submit reports of breaches involving more than 500 individuals.

If fewer than 500 individuals are affected by a breach of unsecured PHI, immediate notification does not need to be made to the Secretary. However, the covered entity must maintain a log or otherwise document the breach and submit the information annually. The information must be submitted to the Secretary no more than 60 days after the end of a calendar year. Again, information on the manner of reporting breaches may be found on the HHS website.

Notification by a Business Associate

A business associate shall, following the discovery of a breach of unsecured PHI, notify the covered entity of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

Notification by a business associate shall include the following:

1. The identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach; and

2. Any other available information that the covered entity is required to include in its notification to the individual.

Law Enforcement Delay

If a law enforcement official states to a covered entity or business associate that a required notification, notice, or posting would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

A policy and procedure related to breach notification is attached as Exhibit M.

PENALTIES FOR INAPPROPRIATE USE OR DISCLOSURE

HITECH increased the penalties for violations of HIPAA by either a covered entity or business associate. The HHS will conduct periodic audits of covered entities and business associates, even if no complaint has been filed. An audit is required if the preliminary investigation of a complaint indicates willful neglect by the covered entity or business associate. According to Section 160.402(c)(2), not only is a business associate subject to penalties for its own HIPAA violations, but:

> [A] business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

Importantly, an agency relationship may be found to exist regardless of whether any formal business associate agreement has been established.

HIPAA also authorizes state attorneys general to bring civil actions in federal courts on behalf of the state residents who have been threatened or adversely affected by a covered entity or business associate that has violated HIPAA.

HIPAA and its implementing regulations also implement a tiered approach to civil monetary penalties. The Secretary of HHS has the authority to impose the following penalties for violations of HIPAA:

Tier 1: Civil monetary penalties of $145 - $73,011 per violation if the covered entity or business associate did not know (and by exercising reasonable diligence[9] would not have known) that the covered entity or business associate violated HIPAA;

Tier 2: Civil monetary penalties of $1,461 - $73,011 per violation if violation was due to reasonable cause[10] and not willful neglect[11]; and

Tier 3: Civil monetary penalties for violations due to willful neglect. If the violation is corrected within 30 days of the date the covered entity or business associate liable for the penalty knew or should have known by the exercise of reasonable diligence, the penalty is $14,602 - $73,011 per violation. If the violation is not corrected within the 30-day period previously described, the penalty is $73,011 per violation.

---

[9] Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

[10] Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated a provision, but in which the covered entity or business associate did not act with willful neglect.

[11] Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the provision violated.

The total amount of penalties for identical violations during a calendar year may not exceed $2,190,294.[12]

The Secretary of HHS may consider certain mitigating factors when making an ultimate determination as to the total amount of civil monetary penalties to be assessed against a covered entity or business associate. These factors include:

1. The nature and extent of the violation, including:
    A. Number of individuals affected;
    B. Time period of the violation.
2. The nature and extent of the harm resulting from the violation, including:
    A. Physical harm;
    B. Financial harm;
    C. Harm to an individual's reputation;
    D. Hindrance of an individual's ability to obtain health care.
3. The history of prior compliance with HIPAA by the covered entity or business associate, including:
    A. Similarity of current violation to any previous noncompliance;
    B. Extent to which the covered entity or business associate attempted to correct any previous noncompliance;
    C. Responsiveness to prior complaints and required compliance efforts.
4. The financial condition of the covered entity or business associate, including:
    A. Whether financial difficulties affected the entity's ability to comply;
    B. Whether monetary penalties would jeopardize the entity's ability to continue to provide, or to pay for, health care;
    C. Size of the covered entity or business associate.

In addition, the Privacy Standards provide for criminal penalties in relation to certain types of violations of the statute that are done knowingly: up to $50,000 and one year in prison for obtaining

[12] The penalty amounts shown are from 91 Fed. Reg. 3665 (Jan. 28, 2026). The penalty amounts are adjusted annually for inflation, and adjusted amounts are published in the Federal Register.

or disclosing PHI; up to $100,000 and five years in prison for obtaining or disclosing PHI under false pretenses; and up to $250,000 and ten years in prison for obtaining PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

It is important that a covered entity enforce sanctions for violations of the Privacy Standards. Failure to do so may result in application of the above penalties to the covered entity and those responsible for enforcing its privacy policies. A policy and procedure related to violations is attached as Exhibit N.

INTRODUCTION TO THE HIPAA SECURITY STANDARDS

On February 20, 2003, the Department of Health and Human Services (HHS) issued regulations (the Security Standards) implementing the provisions of HIPAA that require covered entities to safeguard the security and integrity of electronic protected health information (EPHI). The Security Standards are codified at 45 C.F.R. § 164.308-.312. Furthermore, under HITECH Act, the requirements of the Security Standards also apply to business associates that create, transmit, or maintain EPHI on behalf of a covered entity.

The Security Standards govern covered entities and their business associates when they create, transmit, and maintain PHI in an electronic format (unlike the Privacy Standards, which cover PHI in any format). Specifically, the Security Standards provide standards in three categories: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. Within these categories, the Security Standards do not always prescribe the exact measures that a covered entity must take to implement a safeguard. Therefore, to determine the appropriate measures, the entity should consider its size, technical infrastructure, and resources, and the risk that EPHI may be improperly used or disclosed. Some of the requirements of the Security Standards are designated as "Addressable." A covered entity must implement an addressable requirement unless the entity can document why the requirement is neither reasonable nor appropriate. Exhibit W2 provides guidance on determining the reasonableness and appropriateness of particular addressable requirements. Covered entities must document the measures they take to comply with the Security Standards. This documentation may be in an electronic format and must be retained for six years. This Manual provides a brief overview of some of the key requirements in each category of safeguards and suggests implementation measures. However, the Practice should periodically review the Security Standards and determine the appropriateness of the various safeguards, including any addressable safeguards.

Administrative Safeguards

A covered entity must adopt policies and administer procedures that ensure the integrity, confidentiality, and availability of EPHI. In the category of Administrative Safeguards, HHS mandates that each covered entity implement a security management process that enables it to detect and address security risks. In response to this assessment, the entity will adopt a HIPAA Security Compliance Program and designate a Security Officer to administer the program. In this Manual and the related policies, "HIPAA Security Compliance Program" refers to the policies, procedures, and protocols adopted by the Practice to safeguard EPHI. As part of the program, the entity will ensure that each individual in the workforce has appropriate access to EPHI. Furthermore, the workforce will undergo training on how to comply with security measures. To ensure the adequacy of the program as time passes and as technology advances, the entity must (i) track both successful and attempted security breaches; (ii) develop a plan to address emergency situations; and (iii) periodically evaluate the program. Finally, the covered entity must ensure that business associates that process EPHI on behalf of the entity also comply with the Security Standards.

1. Security Management Process

Each covered entity must determine its organizational weaknesses that leave EPHI vulnerable to improper use or disclosure. The covered entity must address the identified risks by implementing appropriate policies and procedures, tracking the workforce's interaction with EPHI and sanctioning employees who fail to comply with the policies and procedures.

A. Risk Analysis. The Security Standards do not dictate the steps of an entity's risk analysis. Depending on the size and resources of the organization, the covered entity may use questionnaires, conduct on-site interviews, review documents, or utilize automated scanning tools to gather information necessary for the risk analysis. We suggest that your organization implement and document a policy requiring periodic risk assessments including the following steps:

i. Inventory the locations, devices, and information technology (IT) systems that have access to EPHI.

ii. For each location, device, and system, identify the weaknesses that pose a risk to the integrity, confidentiality, and availability of EPHI. To complete this step, consider the likelihood of human threats (such as hackers, computer thieves, and negligent or disgruntled employees); natural disasters (such as fires, earthquakes, and floods); and environmental failures (such as power outages and liquid leakages).

iii. Review and update the protocols for these locations that prevent unauthorized alteration, ensure confidentiality, and protect availability of EPHI.

iv. Determine whether the established protocols satisfy the standards set forth in the Security Standards. Exhibit W3 provides a checklist of these standards.

v. Depending on (i) the impact on EPHI if the weakness was exploited and (ii) the likelihood that the recognized threat will occur, label the risk as high, medium, or low.

vi. Document the results of the assessment.

vii. Review and approve the results. The persons charged with this responsibility should be independent of the personnel conducting the risk assessment.

Section 164.308(a)(1)(ii)(B) of the Security Standards requires covered entities to "[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level." Accordingly, a covered entity should ascertain measures the organization will need to take to comply with the Security Standards and reduce the risks labeled medium and high in the risk analysis. Many entities will be able to incorporate these measures into an existing security program. Finally, the entity should document the measures it adopts in response to the risk analysis.

B. Sanction Policy. Section 164.308(a)(1)(ii)(C) of the Security Standards requires covered entities to sanction "workforce members who fail to comply with the security policies and procedures of the covered entity." To comply with this requirement, a covered entity may amend existing sanction policies to address violations of the security program. Alternatively, the entity may develop a separate sanction policy. Either way, your entity should ensure that the sanction (e.g., reprimand, termination, etc.) varies depending on the severity of the violation and that sanctions will apply equally to all members of the workforce. Further, to provide proper notice to the workforce, your organization should require members to sign a form acknowledging the entity's security measures and the sanctions for non-compliance.

C. Information System Activity Review. Each covered entity must have IT systems that can alert the entity to unauthorized use or disclosure of EPHI. To comply with this standard, your entity should review its systems' capabilities and implement audit and review functions. Also, the entity should establish a written policy requiring periodic review of the audit reports. Some entities may choose to undergo a single annual audit, while others will audit portions of the organization throughout the year. In addition to determining when to review audit reports, an entity should address other issues: (i) will the entity use a third-party, the operating system, or software to conduct the audit; (ii) what activities will the entity track – access to, creation of, editing, and/or deletion of EPHI; (iii) what information will be provided on the audit report (e.g., date, time, and username); and (iv) who is responsible for reviewing audit reports?

2. Assigned Security Responsibility

The Security Standards require each covered entity to assign the responsibility of implementing the HIPAA Security Compliance Program to an individual. However, the rule allows entities to determine the specific functions of and qualifications for the position. Because of the nature of the position, a covered entity should appoint a person who has full understanding of the organization's services and how the organization delivers them. Also, a person with a technology background may be useful to the organization. Thus, some covered entities may assign the duty of Security Officer to the same individual who serves as Chief Information Officer in the IT department. Other entities may determine that the

Privacy Officer should also serve as the Security Officer. We suggest that your entity draft a job description for the Security Officer that includes the following functions:

- Serve as the point of contact for the HIPAA Security Compliance Program;
- Manage implementation of the program;
- Communicate the program's policies and procedures to the workforce;
- Administer the risk analysis;
- Determine IT security investments and purchases;
- Ensure that the program addresses security risks; and
- Implement periodic security evaluations and review the results.

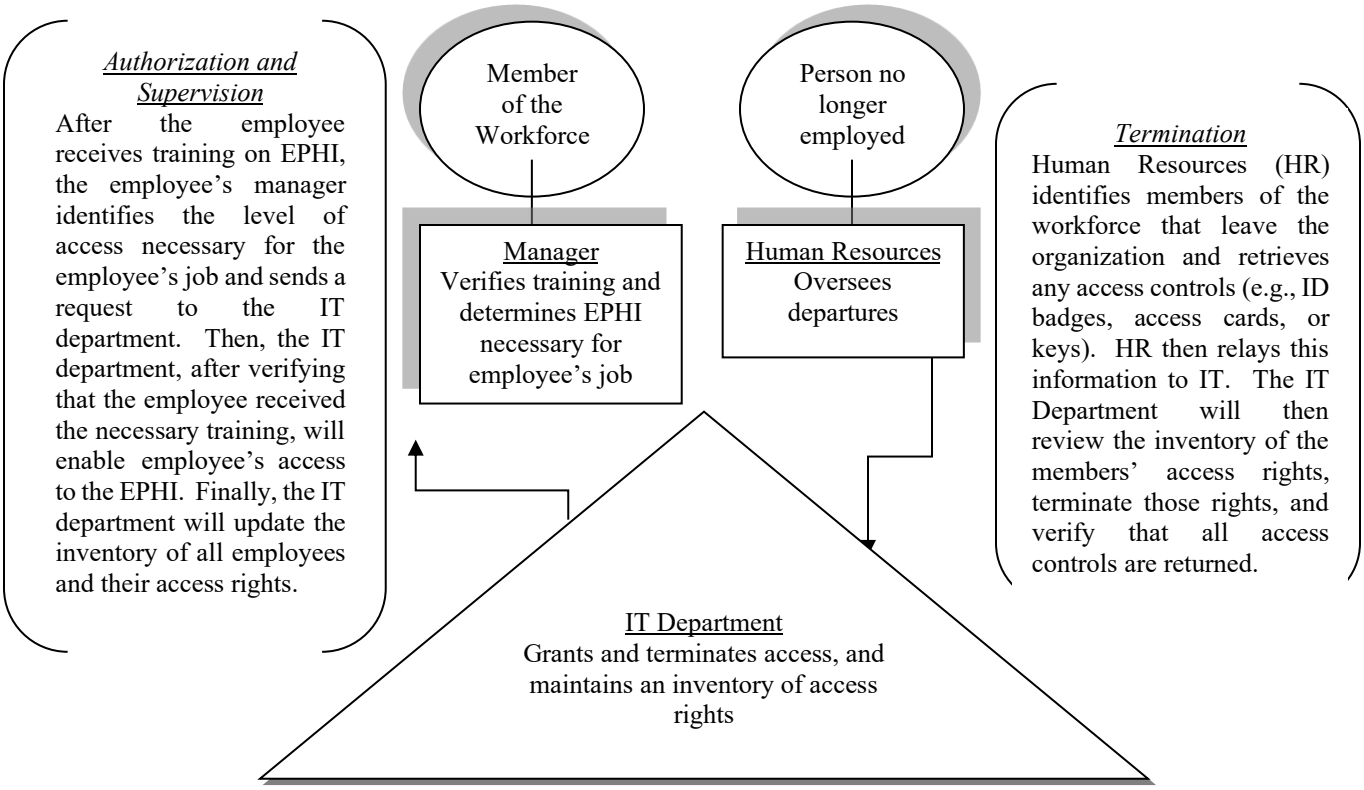
Your organization should also determine who should oversee the work of the Security Officer and include a reporting requirement in the Officer's job description.

3. Workforce Security

Under this standard, a covered entity ensures that members of the workforce have appropriate access to EPHI. A covered entity should develop methods to supervise locations and systems where such information is available, to authorize each workforce member's access to EPHI and to ensure that members of the workforce have a level of access appropriate to their responsibilities. Finally, the Security Standards require covered entities to adopt procedures to terminate workforce members' access.

A. Authorization and/or Supervision, Workforce Clearance Procedure, and Termination (Addressable)

When the organization adds a new workforce member, the entity must provide that individual with access to EPHI to the extent appropriate for his or her job. The Security Standards require entities to adopt and to implement written procedures detailing the authorization process for the workforce's access to EPHI. Likewise, an organization must have a procedure for terminating an individual's access to EPHI when the person is no longer an employee or person's arrangement with the organization is terminated. Additionally, these procedures should address the authorization and termination of business associates' access rights. Many organizations that have IT departments delegate authorization and termination responsibilities to those departments. An IT department will grant and terminate access to EPHI and maintain an inventory of the access rights assigned to each employee and business associate. The diagram below illustrates one example of a procedural model that your entity may adopt to comply with the authorization and termination requirements.



4. Information Access Management

Section 164.308(a)(ii) of the Security Standards requires covered entities to implement procedures to control the workforce's access to EPHI. The Security Standards also require organizations to determine whether any personnel perform clearinghouse functions—that is, whether employees receive PHI from one or more other covered entities and format the PHI into a standardized form. (For example, a covered entity that provides billing services for another entity performs clearinghouse functions.) If so, then the covered entity must adopt policies and procedures that prevent improper disclosure of EPHI from the clearinghouse personnel to the remainder of the organization.

5. Security Awareness and Training

Each covered entity must have a program that informs the organization and its members of anticipated security risks and appropriate responses. To meet this standard, entities should implement the Security Standards' four addressable requirements: (i) periodically update the workforce on security issues; (ii) protect against malware; (iii) monitor the workforce's log-in attempts; and (iv) adopt procedures to create and change passwords. When adopting a security program appropriate for your organization, consider the following measures:

A. Security Reminders – The Security Officer should ensure that the workforce has access to the entity's current security policies and procedures. Furthermore, the officer should periodically distribute emails or

memoranda addressing topics relevant to the organization's needs and explaining noteworthy security policies.

B. Protection From Malicious Software – All equipment (computers, laptops, smart phones, portable devices, etc.) that can access EPHI should have software that will detect, report, and protect against malicious software. Thus, the persons responsible for IT should install and regularly update firewall and virus protection software on electronic devices.

C. Log-in Monitoring – The IT system should deny a user access to EPHI after a specified number of unsuccessful log-in attempts. Your entity may decide to vary the number of allowable attempts depending on the criticality of the information the user seeks to access.

D. Password Management – Passwords should contain both numbers and letters and should be changed periodically (e.g., every 90 days). If your organization has the technological resources to force periodic password changes, then enable this feature. To make the log-in process more robust, add a second authentication requirement. For example, you may require users to answer a security question. Finally, your organization may need to adopt a log-in process for remote access users. Remote Authentication Dial-In User Service (RADIUS) is an example of a tool that can screen remote access users.

6. Security Incident Procedures

Security incidents include unauthorized access to or use, disclosure, modification, or destruction of PHI and interference with operations of information systems, whether successful or only attempted. Also, viruses, spyware, worms, and Trojan horses that threaten system crashes qualify as security incidents. The Security Standards require entities to detect and respond to security incidents. To comply with this requirement, organizations should monitor alerts from antivirus software, watch for the appearance of filenames with unusual characters on the system, and monitor failed log-in attempts. Also, the organization should develop a reporting template so that the workforce may report any security incidents, such as loss or exposure of EPHI. By tracking threats of security incidents, the entity may identify weaknesses in the system and protect against security breaches.

When a security incident occurs, the entity should (i) inventory the systems and information affected by the incident, (ii) identify the source of the incident, and (iii) if the incident was successful, investigate why existing protective measures did not prevent it. This investigation will determine how the organization should respond. In some cases, the organization may need to notify individuals, the HHS Secretary, and possibly the media. In other cases, the organization may need to revise the security program to prevent future incidents. Regardless of the end result, entities should document each step of the investigation and response process.

7. Contingency Plan

The Security Standards require the establishment of written protocols that identify how the entity will respond if disaster strikes (e.g., "fire, vandalism, system failure, and natural disaster"). To comply with this requirement, an entity should first identify the hardware, software, and personnel that are critical to business operations. Then brainstorm alternative methods that the business could employ in case these critical elements become unavailable. Accordingly, the entity should incorporate feasible and cost-effective methods into a written contingency plan. This plan should (i) identify who will determine when the entity must operate under the contingency plan; (ii) establish procedures that protect the security of EPHI when the business operates under the alternative method; (iii) determine how EPHI will be accessed; and (iv) contain procedures for restoring lost data.

To enable the restoration process, the entity should train the workforce on backup procedures. Larger entities may require the workforce to save files on a network, while smaller entities may implement a policy mandating periodic backup on external media. Furthermore, entities need to designate personnel with the authority to access and to restore systems when necessary. Finally, the Security Standards require entities to periodically test their contingency plans. We suggest an annual evaluation of whether the contingency plan will successfully enable continued business operations and ensure the security of EPHI in a disaster situation.

8. Evaluation

Covered entities must annually evaluate the effectiveness of their security program. This evaluation should address both technical safeguards, such as firewalls and anti-virus software, as well as non-technical procedures like the workforce training program. Also, the Security Officer should conduct additional evaluations when the officer determines that changes in business operations may affect the safety of EPHI.

9. Business Associate Contracts and Other Arrangements

Covered entities and their business associates must sign Business Associate Agreements (BAAs) ensuring the security of EPHI communicated between the parties. Covered entities should have BAAs already in place as required by the Privacy Standards and can amend those agreements to incorporate the requirements of the Security Standards. In addition to the provisions required under the Privacy Standards, covered entities should ensure that each BAA contains:

- A clause requiring the business associate to develop a security program that includes a periodic risk assessment and to safeguard any EPHI;
- Reporting requirements that oblige the business associate to inform the covered entity of results from the risk assessment and any exposure or loss of EPHI;

- An assurance that the business associate will obtain satisfactory assurances that any subcontractor will appropriately safeguard EPHI;
- A provision enabling the covered entity to inspect the business associate's operations to ensure the security of EPHI; and
- A clause authorizing the covered entity to terminate the agreement if the business associate violates a material term.

Physical Safeguards

The Security Standards require each covered entity to implement policies and procedures that address the physical arrangement of its buildings and technological systems. Many organizations may have policies in place that sufficiently meet the following requirements. Therefore, entities should review current operations and determine whether they need to adopt any further procedures to comply with the Physical Safeguards required under the Security Standards.

1. Facility Access Controls

Each covered entity must "[i]mplement policies and procedures to limit physical access to its electronic information systems." § 164.310(a)(1). To comply with this requirement, an entity should first inventory all physical spaces where one could access EPHI. If employees have remote access privileges, this inventory will include the employees' homes as well as the entity's offices. A complete inventory will also include the technology devices located in the physical space. For the office building, the covered entity should, at minimum, ensure that doors to areas not open to the public remain locked. An organization may decide to employ further precautions such as surveillance cameras or signs warning against unauthorized access to technology systems.

In addition to controlling the doors to the physical space, covered entities must also monitor the persons that access the physical space. Accordingly, organizations may require employees to wear identification tags. When monitoring visitors, an entity may require visitors to check in with reception or to wear name badges. Alternatively, the entity could assign visitor escorts. Finally, the Security Standards require entities to monitor personnel that access the physical space to repair or to modify technology systems. Each entity should maintain a log of maintenance and repair visits, recording the identity of each visitor and the purpose of the visit.

2. Workstation Use and Security

We suggest that entities tag electronic equipment so that any lost or stolen device may be tracked back to the entity. Consider employing locking mechanisms to further protect portable devices. At minimum, entities should arrange devices so that unauthorized persons cannot view any displays of EPHI. Likewise, entities need to train remote users to use care in arranging devices that access EPHI.

To ensure proper use of workstations, an entity should determine the scope of allowable use for each computing device. This determination should be effectively communicated to the workforce via a training program or posted signs.

3. Device and Media Controls

Under this section of the Security Standards, entities must develop policies and procedures for the proper use of memory devices that are either transportable from or attached to electronic computing devices, such as discs, memory sticks, and hard drives. First, entities are required to account for all such devices. To comply with this requirement, we suggest that entities limit employees' rights to use transportable memory devices. For employees who have the right to store EPHI on memory devices, the entity should purchase and assign the devices to the employees, so that the entity can keep an inventory of the memory devices and their assigned use.

Under the Media Control section, the Security Standards require entities to develop procedures to remove all EPHI from memory devices when the devices are either recycled or destroyed. If a device is slotted for destruction, the entity may simply employ enough physical force to render any EPHI irretrievable from the device. Degaussing will also remove EPHI from magnetic media. This is a method whereby a strong magnetic field erases data from a device. When an entity donates devices or moves them to other departments in the organization, the entity must delete the EPHI stored on the devices. Therefore, in your policies and procedures, delegate the deletion responsibility to appropriate persons and ensure documentation of the activity.

Technical Safeguards

Under the Technical Safeguards section of the Security Standards, entities implement practices and technology operations to ensure that only authorized personnel and software programs access EPHI. This section requires entities to implement technology that will protect the authenticity of EPHI and secure the information during transmission. Also under this section, entities must regulate access to and audit the use of EPHI.

1. Access Controls

To govern the workforce's access to EPHI, entities should require each member to have a unique username and password. An entity may either assign the username or set standards for member generated usernames. Standards for usernames may be similar to those for passwords (e.g., requiring a specified number of characters and an alpha-numeric combination). Also, for systems in which the security of EPHI is at risk, entities may want to implement two-level authentication, such as password authentication plus a security question.

The Security Standards include addressable standards concerning encryption and automatic logoff technology. Encryption solutions include secure socket layer (SSL) and hypertext transfer protocol secure (HTTPS). The Security Standards do not designate the

length time before user inactivity should result in automatic logoff. Depending on the entity's resources, an entity may establish different time limits based on the criticality of the EPHI and the system in use.

2. Integrity Controls

Entities must ensure the authenticity of EPHI both while it is stored and when it is transmitted. Various tools are available for entities to protect the authenticity of EPHI, including:

- SSL secured connections for emails;
- Error-correcting memory;
- Digital signatures;
- Checksum technology;
- Message level standards, such as PGP, PEM, SET, or S/MIME.

Organizational Requirements

A business associate agreement must provide for certain provisions or guarantees. First, the agreement must provide that the business associate will comply with the Security Standards. Second, a business associate must ensure that its contract or other arrangements with a subcontractor complies with the Security Standards. Lastly, under the contract or arrangement, a business associate is responsible to report to covered entities any security incident of which it becomes aware, including breaches of unsecured PHI. Consider the following example described by the OCR within its preamble comments:

> [U]nder these provisions, a business associate contract between a business associate and a business associate subcontractor would need to provide that the subcontractor report any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410, to the business associate. This would mean that if a breach of unsecured protected health information occurs at or by a second-tier subcontractor, the subcontractor must notify the business associate subcontractor with which it contracts of the breach, which then must notify the business associate which contracts with the covered entity of the breach, which then must notify the covered entity of the breach. The covered entity then notifies the affected individuals, the Secretary, and, if applicable, the media, of the breach, unless it has delegated such responsibilities to a business associate.

EXHIBITS

Exhibit A1
Form

CHILDREN'S DENTISTRY OF AMARILLO
NOTICE OF PRIVACY PRACTICES

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

Children's Dentistry of Amarillo is required by law to maintain the privacy of certain health information about you, to notify affected individuals following a breach of unsecured protected health information, and to inform you of its practices with respect to the privacy of that information. This Notice of Privacy Practices is being provided to inform you of the ways that we may use the personal information we collect or receive about you and how we may disclose that information.

Federal and state laws require health care providers to protect the privacy of information about your health, your health care, and payment for your health care, if that information identifies you or could be used to identify you. The law permits us to use or disclose your protected health information only for certain specific purposes, unless you give us a written authorization permitting us to make other uses and disclosures. This notice describes the purposes for which we may use or disclose protected health information about you.

The law also gives you certain rights with respect to your protected health information. This notice provides a summary of those rights.

USES AND DISCLOSURES FOR TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

We may use and disclose health information, including the disclosure of health information electronically, about you without your specific authorization for purposes of treatment, payment and health care operations.

Treatment - We may use your health information to treat you and share it with other professionals who are treating you. Example: we may share your dental records with another dentist who is treating you.

Payment - We may use and disclose health information for activities required to obtain payment from you or your insurance carrier for the services we provide to you. Example: we may share information about you to your dental insurance plan for eligibility determination, pre-certification, billing and collection.

Health care operations - We may use and share your health information to run our dental practice, improve your care, and contact you when necessary. Example: we may use health information about you to manage your treatment and services.

OTHER USES AND DISCLOSURES THAT DO NOT REQUIRE AUTHORIZATION

There are a limited number of other purposes for which we may use or disclose your health information without a written authorization from you.

- We may use or disclose protected health information when the use or disclosure is required by law.
- We may use or disclose protected health information to avert a serious threat to your health or safety, or the health and safety of others.
- We may use or disclose protected health information for certain public health activities, such as reporting certain communicable diseases, or reporting information to the Food and Drug Administration about treatments that are regulated by that agency.
- We may use or disclose protected health information for workers' compensation claims.
- We may use or disclose protected health information for health research.
- We may disclose protected health information to a legally authorized government authority, such as a social service or protective services agency, if we reasonably believe you are a victim of abuse, neglect or domestic violence.
- We may disclose protected health information to agencies authorized by law to conduct health oversight activities, such as licensing, inspections, and audits.
- We may disclose protected health information in response to court orders or subpoenas, and for certain law enforcement purposes.
- We may disclose protected health information to coroners, medical examiners and funeral directors to enable them to carry out their duties.
- We may disclose protected health information to organizations that are involved in arranging for donation or transplantation of tissue and organs.
- We may disclose protected health information to authorized government agencies when necessary for national security or intelligence purposes, or for certain military and veteran's activities.
- We may disclose protected health information to attorneys, accountants, and others acting on our behalf, provided they have signed written contracts agreeing to protect the confidentiality of the information.
- Unless you object, we may disclose to a member of your family, another relative, a close personal friend, or any other person identified by you, the protected health information directly relevant to that person's involvement with your health care or payment for your health care.

USES AND DISCLOSURES WITH YOUR AUTHORIZATION

We must obtain your prior authorization for [uses and disclosures of psychotherapy notes (where appropriate),] uses and disclosures of your protected health information for marketing purposes, and any sale of your protected health information. We will obtain your authorization for any use or disclosure of your protected health information for purposes other than those summarized

above. You may revoke an authorization at any time, except to the extent we have acted in reliance on the authorization, by sending a written notice of revocation to the address on the last page of this notice.

YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION

You have the following rights concerning your protected health information. You may exercise these rights by sending a written request to the address on the last page of this notice.

- You may request additional restrictions to the use or disclosure of your protected health information for treatment, payment or health care operations. However, in most cases we are not required to agree to the requested restrictions. [Health care providers only: We are required to agree to a request to restrict disclosure of your protected health information to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which you have paid out of pocket in full.]
- We normally contact you by telephone or mail at your home address. You may request that we contact you at some other address or telephone number, or by some other method, such as e-mail. We will accommodate reasonable requests.
- You may inspect and obtain a copy of protected health information that is used to make decisions about your care or payment for your care. We may deny a request to inspect records only in a few limited circumstances. If you request copies of records, we may charge you a reasonable fee for the copies.
- You have the right to request amendment of the protected health information we maintain about you. We may deny your request if we determine that the record is accurate and complete, or if we did not create the record, unless the creator of the record is no longer available, or if you do not have a right to access the record. If we deny your request, you have the right to submit a statement disagreeing with our decision and to have the statement attached to the record.
- You may request an accounting of certain disclosures we have made of your protected health information. The accounting is not required to include disclosures for treatment, payment, or health care operations, disclosures to persons involved in your health care or payment, disclosures for notification purposes, or disclosures with your written authorization. You may receive one accounting free of charge within a 12-month period. We may charge a reasonable fee for all subsequent requests during the same 12-month period.
- You have the right to receive notification in the event of an unpermitted use or disclosure of your unsecured protected health information which compromises the security or privacy of your information.
- You have the right to obtain a paper copy of this notice upon request.

SUBSTANCE USE DISRODER (SUD) RECORDS

In the unlikely event that we receive SUD Records about you from a SUD treating provider, certain uses and disclosures that are permitted under HIPAA are limited by 42 CFR Part 2. We may not use or disclose SUD Records for any criminal investigation of a patient or for use in any civil, criminal, administrative, or legislative proceedings against a patient.

AMENDMENT OF THIS NOTICE

We reserve the right to change the terms of this Notice of Privacy Practices, and to make the new notice provisions effective for all protected health information that we maintain. If we amend the terms of this notice. We will post the revised Notice on our website. You may also obtain a copy of the revised Notice by sending a request to the address below.

FOR MORE INFORMATION OR TO REPORT A PROBLEM

If you have questions or would like additional information about our privacy practices, please call or write:

Children's Dentistry of Amarillo
4501 Van Winkle Dr.
Amarillo, TX 79119
Attn: Corporate Privacy Officer
Telephone: 806-994-4184

If you believe that your privacy rights have been violated, you may file a written complaint at the address above. You may also file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting **www.hhs.gov/ocr/privacy/hipaa/complaints/.**

We will not retaliate against you for filing a complaint.

This Notice of Privacy Practices is effective February 16, 2026.

NOTICE INFORMING INDIVIDUALS ABOUT NONDISCRIMINATION AND ACCESSIBILITY REQUIREMENTS

Discrimination is Against the Law

Children's Dentistry of Amarillo complies with applicable federal civil rights laws and does not discriminate on the basis of race, color, national origin, age, disability, or sex. Children's Dentistry of Amarillo does not exclude people or treat them differently because of race, color, national origin, age, disability, or sex.

Children's Dentistry of Amarillo:

- Provides free aids and services to people with disabilities to communicate effectively with us, such as:
    - Qualified sign language interpreters
    - Written information in other formats (large print, audio, accessible electronic formats, other formats)
- Provides free language services to people whose primary language is not English, such as:
    - Qualified interpreters
    - Information written in other languages

If you need these services, contact our Treatment Coordinator.

If you believe that Children's Dentistry of Amarillo has failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, or sex, you can file a grievance with:

Treatment Coordinator
4501 Van Winkle Dr., Amarillo, TX 79119
806-994-4184
[Fax]
[Email]

You can file a grievance in person or by mail, fax, or email. If you need help filing a grievance, our Treatment Coordinator, is available to help you.

You can also file a civil rights complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, electronically through the Office for Civil Rights Complaint Portal, available at https://ocrportal.hhs.gov/ocr/portal/lobby.jsf, or by mail or phone at:

U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201
1-800-368-1019, 800-537-7697 (TDD)

Complaint forms are available at http://www.hhs.gov/ocr/office/file/index.html.

Exhibit A2
Policy and Procedure

POLICY TITLE: Privacy: Notice of Privacy Practices	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations issued under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of protected health information (PHI) maintained by Children's Dentistry of Amarillo. In particular, the purpose of this policy and procedure is to ensure compliance with HIPAA regulations related to Notice of Privacy Practices.

POLICY

Children's Dentistry of Amarillo must provide a Notice of Privacy Practices containing both a notice of nondiscrimination and the availability of language services in accordance with Section 1557 of the Patient Protection and Affordable Care Act to each patient as required by HIPAA regulations. The Notice of Privacy Practices will explain to patients how Children's Dentistry of Amarillo may use and disclose the patient's PHI obtained by Children's Dentistry of Amarillo in the course of providing services to the patient.

SOURCE

45 C.F.R. § 164.520

PROCEDURE

1. The Notice of Privacy Practices must be provided to all new patients at the time of initial delivery of services.

2. The patient should sign an Acknowledgment verifying receipt of the Notice of Privacy Practices. Children's Dentistry of Amarillo shall provide an Acknowledgment to patients with the Notice of Privacy Practices. Children's Dentistry of Amarillo will make a good faith effort to see that the Acknowledgment is returned.

3. If Children's Dentistry of Amarillo does not receive a signed Acknowledgment within 30 days of providing the Notice of Privacy Practices, it shall call and inform the patient that it is forwarding an additional Notice of Privacy Practices and Acknowledgment and explain the importance of returning the Acknowledgment. These efforts shall be repeated at 60 days and 90 days if the Acknowledgment is not returned.

4. At the end of 120 days, the Privacy Officer shall review the documentation of the efforts to obtain a signed Acknowledgment and, if applicable, will determine if a good faith effort has been made. If the documentation does not show a good faith effort, the Privacy Officer will direct additional efforts to be made.

5. If a patient refuses to sign an Acknowledgment, such action should be documented in the patient's medical record and the Privacy Officer notified.

6. If there is a change to the Notice of Privacy Practices, Children's Dentistry of Amarillo will provide a copy of the revised Notice to a patient upon the patient's request.

7. Children's Dentistry of Amarillo shall, at all times, post a copy of its Notice of Privacy Practices on its website.

8. Children's Dentistry of Amarillo shall post its Notice of Privacy Practices in a conspicuous location at each location where services are provided.

Exhibit A3

Children's Dentistry of Amarillo

Acknowledgment of Notice of Privacy Practices

Attached is Children's Dentistry of Amarillo's Notice of Privacy Practices (the "Notice"), which describes how we use and disclose your health information. By printing and signing your name on this cover sheet, you are agreeing that you have received a copy of the Notice on the date and time indicated below.

If you have any questions regarding the information set forth in the Notice of Privacy Practices, please do not hesitate to contact our Privacy Officer at 806-994-4184.

Name: _____

Signature: _____

Date and Time Notice Received: _____

Witness name (if refused by patient): _____

Legally Authorized Representative: _____

Relationship to Patient: _____

Acknowledgment of Notice of Privacy Practices	**Patient Identification**

Exhibit B
Policy and Procedure

POLICY TITLE: Privacy: Privacy Individual Access	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure that Children's Dentistry of Amarillo complies with federal regulations enacted pursuant to the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of protected health information (PHI). In particular, the purpose of this policy is to ensure that patients are granted the right to access their own medical records as required by HIPAA.

POLICY

Children's Dentistry of Amarillo will allow a patient access to his or her own medical records in accordance with HIPAA.

SOURCE

45 C.F.R. § 164.524

PROCEDURE

1. Patients may request access to the PHI maintained by Children's Dentistry of Amarillo. Patients may also request Children's Dentistry of Amarillo to transmit a copy of the PHI directly to another person designated by the individual. All requests must be made in writing to the Privacy Officer. Requests for disclosure to another person must be signed by the individual and clearly identify the designated person and where to send the copy of the PHI. All patients who request access to their PHI will be granted such access unless HIPAA or other law allows for the denial of access.

2. As mandated by HIPAA, within 30 days of the receipt of a written request for access, unless a more restrictive state statute applies, Children's Dentistry of Amarillo will provide a written response to the request. A copy of the written response shall be maintained in the patient's medical record.

A. Under Texas law, if Children's Dentistry of Amarillo is using an electronic health records system that is capable of fulfilling the request, Children's Dentistry of Amarillo will provide the requested record in electronic form to the patient within 15 business days.

3. The written response will indicate that the request has been received, will be approved by the Privacy Officer prior the being sent to the patient, and, either:

   A. Indicate that access has been granted:

      i. A copy of the records will then be provided; or

      ii. Information regarding the time and place to access the PHI will be provided.

   B. Indicate that access has been denied in whole or in part:

      i. Information indicating justification for the denial will be provided; and

      ii. A copy of the denial justification will be forwarded to the Privacy Officer.

4. If Children's Dentistry of Amarillo is unable to respond to the request for access within 30 days, Children's Dentistry of Amarillo may have an additional 30 days to respond, provided:

   A. The patient receives information detailing the reason for the delay and estimated date that the request will be completed; and

   B. Children's Dentistry of Amarillo may only extend the response time once per request.

5. Children's Dentistry of Amarillo will provide PHI in the form or format requested by the patient, unless the PHI is not readily producible in the requested form or format. In such case, the PHI must be produced in a readable hard copy form or such format as agreed to by Children's Dentistry of Amarillo and the patient.

   A. However, if the PHI is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Children's Dentistry of Amarillo will provide the individual with 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 the covered entity and the individual.

6. If the patient agrees in advance, a summary or explanation of the PHI may be provided instead.

7. A reasonable, cost-based fee, for supplying copies, summaries or explanations of PHI may be imposed provided the fee only includes cost of copying the PHI, whether in paper or electronic form, requested by the patient including the cost of supplies for and labor of copying.

8. The patient may be charged for postage when the patient requests the copy, summary or explanation of PHI be mailed.

9. If agreed to in advance, a reasonable fee may be charged for preparing an explanation or summary of the PHI requested by the patient.

DENYING ACCESS

All denials of access must be approved in advance by Children's Dentistry of Amarillo's Privacy Officer.

DENIALS THAT ARE NOT SUBJECT TO THE RIGHT OF REVIEW

1. Children's Dentistry of Amarillo may deny patient access to PHI, without the right to a review, for the following reasons:

   A. The information was compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding;

   B. The provider is acting under the direction of a correctional institution;

   C. The information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information; or

   D. The information is subject to restrictions under the terms of the Privacy Act, 5 U.S.C. 552a.

2. If Children's Dentistry of Amarillo denies access for these reasons, Children's Dentistry of Amarillo must:

   A. To the extent possible, give the patient access to any other PHI requested, after excluding the PHI that has been denied; and

   B. Must provide a written denial, within 30 days unless state statutes are more restrictive, indicating:

      i. The basis for the denial;

ii. A statement of the patient's review rights under HIPAA, including a description of how a patient may exercise such rights; and

iii. A description of how and where the patient may register a complaint with Children's Dentistry of Amarillo's Privacy Officer or with the Secretary of HHS.

DENIALS THAT ARE SUBJECT TO THE RIGHT OF REVIEW

1. A patient has a right to have a denial reviewed if access to PHI is denied in the following circumstances:

   A. A licensed health care professional has determined, in the exercise of professional judgment, that granting the requested access is reasonably likely to endanger the life or physical safety of the patient or another person;

   B. The PHI makes reference to another person (unless that person is a health care provider) and granting the requested access is reasonably likely to cause substantial harm to that person, as determined by a licensed health care professional in the exercise of professional judgement; or

   C. The request for access is made by the patient's personal representative and such access is reasonably likely to cause substantial harm to the patient or another person, as determined by a licensed health care professional in the exercise of professional judgement.

2. If a patient is denied access for one of the reasons stated above, the patient has the right to have the denial reviewed by a licensed health care professional who is designated by Children's Dentistry of Amarillo to act as the reviewing official and who did not participate in the original decision to deny access.

3. In the event of such a review hearing:

   A. This licensed health care professional will be Children's Dentistry of Amarillo's dental director; or

   B. In the event Children's Dentistry of Amarillo does not have a dental director, arrangements for review by a licensed health care professional will be made by the Privacy Officer.

4. The reviewing official must make a determination within 30 days.

5. Children's Dentistry of Amarillo is bound by the decision of the reviewing official to provide or deny access. A copy of the reviewing official's decision will be forwarded to the Privacy Officer.

6. The patient must be notified in writing of the decision within 30 days of the reviewing official's decision.

Exhibit C1
Policy and Procedure

POLICY TITLE: Privacy: Tracking Disclosures of Medical Records	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all individually identifiable patient information. In particular, the purpose of this policy is to ensure that Children's Dentistry of Amarillo tracks disclosure of patient health information (PHI) in order to provide the patients with an accounting of disclosures in compliance with the HIPAA regulations.

POLICY

Children's Dentistry of Amarillo shall maintain a record of all disclosures of PHI. In accordance with the HIPAA regulations and Children's Dentistry of Amarillo's policy on Accounting of Disclosures, Children's Dentistry of Amarillo shall, upon the request of a patient, provide the patient with an accounting detailing disclosures of PHI.

SOURCE

45 C.F.R. § 164.528

PROCEDURE

1. Children's Dentistry of Amarillo may only release PHI after obtaining a valid authorization from the patient unless otherwise authorized to make the disclosure by the HIPAA regulations.[13] Release of PHI in violation of this policy will result in disciplinary action up to and including termination.

[13] Refer to policies and procedures for Authorizations.

2. Children's Dentistry of Amarillo shall track release of all PHI subject to an accounting under HIPAA through a PHI Disclosure and Use Log.

3. Information to be tracked includes, but is not limited to:

   A. Patient name;

   B. Date of disclosure;

   C. Name of the entity or person who received the PHI;

   D. Address of recipient;

   E. If applicable, proof of whether the PHI reached the intended recipient, including but not limited to the following:

      i. A tracking number when sent via Federal Express, UPS, or by U.S. Postal Service;

      ii. Facsimile confirmation sheets. All facsimile confirmation sheets should be retained as confirmation that the PHI was received at the correct fax number; or

      iii. E-mail return receipts. Employees must request a return receipt for all e-mail sent with PHI as an attachment.

   F. Brief description of the PHI disclosed; and

   G. Brief statement of the purpose of disclosure.

Exhibit C2
Policy and Procedure

POLICY TITLE: Privacy: Accounting of Disclosure of Medical Records	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulation under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI). In particular, the purpose of this policy is to ensure that upon the request of a patient, Children's Dentistry of Amarillo shall provide the patient with an accounting of disclosures in compliance with the HIPAA regulations.

POLICY

In accordance with HIPAA regulations, Children's Dentistry of Amarillo will, upon the written request of the patient, provide the patient with an accounting of disclosures of PHI.

SOURCE

45 C.F.R. § 164.528

PROCEDURE

1. A patient has the right to receive an accounting of disclosures of PHI made by Children's Dentistry of Amarillo for the six years[14] prior to the date on which the accounting of disclosures is requested. A patient may also request an accounting of disclosures of PHI used for treatment, payment and health care operations for the three (3) years prior to the date on which the accounting is requested. Requests for an accounting shall be received and processed by the Privacy Officer.

2. Children's Dentistry of Amarillo will provide a patient with an accounting within 60 days of receipt of the request. If Children's Dentistry of Amarillo is unable to

[14] However, the patient may request an accounting period of less than six years.

complete the request in the time frame specified, the time period may be extended for not more than 30 days, provided that within the initial 60-day period Children's Dentistry of Amarillo provides the patient with a written statement of the reasons for the delay and the date by which Children's Dentistry of Amarillo will provide the accounting to the patient.

3. The accounting is not required to include disclosures:

   A. To a patient in accordance with the patient's right to access their medical records;

   B. For the facility's directory or to persons involved in the individual's care as provided in accordance with HIPAA;

   C. For national security or intelligence purposes as provided in accordance with HIPAA;

   D. To correctional institutions or law enforcement officials in accordance with HIPAA;

   E. Disclosures that occurred prior to Children's Dentistry of Amarillo HIPAA compliance date;

   F. Disclosures made pursuant to an authorization signed by the patient;

   G. Disclosures incident to a use or disclosure permitted by HIPAA; and

   H. As part of a limited data set in accordance with HIPAA.

4. The accounting must include:

   A. The date of the disclosure;

   B. Name of the entity of person who received the PHI;

   C. The address of such entity or person, if known;

   D. A brief description of the PHI disclosed;

   E. A brief statement of the purpose of the disclosure:

      i. Reasonably informs the patient of the basis for the disclosure; or

      ii. Either of the following:

a. A copy of the patient's written authorization to release the PHI in question; or

b. A copy of a written request for a disclosure under HIPAA:

1) By the Secretary of HHS to investigate Children's Dentistry of Amarillo's compliance.

5. If Children's Dentistry of Amarillo has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting must provide:

A. Information as detailed above including:

i. The frequency, periodicity, or number of the disclosures made during the accounting period; and

ii. The date of the last disclosure during the accounting period.

6. Children's Dentistry of Amarillo will provide the first accounting to a patient in any 12-month period without charge.

7. After the first accounting, Children's Dentistry of Amarillo may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the 12-month period provided:

A. The patient is informed in advance of the fee; and

B. The patient has the opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

Exhibit D
Policy and Procedure

POLICY TITLE: Privacy: Medical Record Amendment(s)	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI). In particular, the purpose of this policy is to ensure that Children's Dentistry of Amarillo complies with HIPAA requirements regarding a patient's right to request amendment of medical records.

POLICY

Children's Dentistry of Amarillo will provide its patient with the opportunity to request amendment(s) to PHI. All requests for amendment(s) will be thoroughly researched prior to acceptance or denial.

SOURCE

45 C.F.R. § 164.526

PROCEDURE

Request for Correction

1. HIPAA gives the patient the right to request an amendment to PHI. Children's Dentistry of Amarillo must permit the patient to request an amendment but is not required to amend the PHI and may deny the request for amendment if it determines that the PHI:

    A. Was not created by Children's Dentistry of Amarillo unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available (i.e. the originating physician is deceased, the hospital is no longer open for service, etc.);

B. Is not part of the dental record set maintained by Children's Dentistry of Amarillo;

C. The requested amendment concerns information that would not be subject to a right to inspect and copy; or

D. Is accurate and complete.

2. Copies of the request for amendment must be forwarded to the Privacy Officer as soon as possible.

3. The Privacy Officer will be responsible for reviewing the request and determining whether the request should be granted.

4. Children's Dentistry of Amarillo will provide the patient with a response to the request for amendment no later than 60 days after the receipt of the request. If unable to act upon the request in 60 days, Children's Dentistry of Amarillo may have one extension of not more than 30 days for each request, provided that within the initial 60-day period, Children's Dentistry of Amarillo provides the patient with a written statement of the reasons for the delay and the date by which Children's Dentistry of Amarillo will complete its action on the request.

Agreeing to Request for Amendment(s)

1. Only the Privacy Officer has the authority to accept or deny an amendment to a patient's medical record.

2. Acceptance of a request for amendment(s) to PHI will be documented in the patient's medical record.

3. Original medical records cannot be altered in any manner.

4. Amendments will only be made by any of the following methods:

A. Stapling the new information to the documentation being amended;

B. Making a copy of the original documentation and making the change(s) to the copy then stapling the copy to the original documentation; or

C. For electronic health records, providing a link to the amendment in the documentation being amended.

5. Children's Dentistry of Amarillo will obtain an authorization from the patient to provide the amendment to persons or entities identified by the patient as having previously received the PHI and to persons or entities that Children's Dentistry of

Amarillo knows may rely on the PHI as well as business associates.[15] This must be done within 30 days of the date on which Children's Dentistry of Amarillo agreed to the amendment.

6. If Children's Dentistry of Amarillo is informed by another health care provider of an amendment to a patient's PHI, Children's Dentistry of Amarillo must amend the PHI it maintains as detailed above.

Denying Request for Amendment(s)

1. Only the Privacy Officer has the authority to accept or deny an amendment to a patient's medical record.

2. Denials for amendment(s) to PHI will be documented in the patient's medical record.

3. The Privacy Officer is responsible for providing the patient with justification for denial of request for amendment.

4. The denial must inform the patient:

   A. That the patient has the right to submit a written statement disagreeing (Statement of Disagreement) with the denial and directions detailing how the patient may submit such a statement;

   B. That, if the patient does not submit a Statement of Disagreement, the patient may request that Children's Dentistry of Amarillo provide the patient's original request for amendment of PHI and the denial with any future disclosures of the PHI that is the subject of the amendment;

   C. That the patient may complain to Children's Dentistry of Amarillo's Privacy Officer including contact information; and

   D. How the patient may complain to the Secretary of the Department of Health and Human Services, including contact information.

5. After having supplied the patient with the justification for the denial of request for amendment as detailed above, Children's Dentistry of Amarillo must permit the patient to submit a written Statement of Disagreement disagreeing with the denial of all or part of the request. Children's Dentistry of Amarillo will not accept a Statement of Disagreement in excess of two (2) pages.

[15] Refer to policies and procedures for business associates.

6. Children's Dentistry of Amarillo may, but is not required to, prepare a written rebuttal to the patient's Statement of Disagreement. The decision to prepare a written rebuttal shall be made by the Privacy Officer. If such rebuttal is prepared:

   A. A copy will be sent to the patient; and

   B. A copy will be retained in the patient's medical record.

7. Children's Dentistry of Amarillo must identify the record or PHI that is in dispute and append the patient's request for amendment, denial to the request by Children's Dentistry of Amarillo , the patient's Statement of Disagreement, if any, and, if applicable, the rebuttal prepared by Children's Dentistry of Amarillo to the record set.

Exhibit E
Policy and Procedure

POLICY TITLE: Privacy: Restrictions on Use	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI). In particular, the purpose of this policy is to ensure that Children's Dentistry of Amarillo complies with HIPAA requirements regarding Children's Dentistry of Amarillo's patients' rights to request additional restrictions to the use of their PHI.

POLICY

In accordance with the HIPAA regulations, Children's Dentistry of Amarillo will allow patients to request restrictions on the use of the patient's PHI by Children's Dentistry of Amarillo.

SOURCE

45 C.F.R. § 164.522

PROCEDURE

1. The patient has the right to submit a request for restrictions to the use of or for confidential communications regarding his or her PHI. All such requests must be made in writing.

2. Upon receipt of a request for restrictions or confidential communications, the request should be immediately forwarded to the Privacy Officer.

3. Children's Dentistry of Amarillo is not obligated to comply with a request for restrictions except in certain situations in which the requested restriction concerns disclosures to a health plan. Children's Dentistry of Amarillo must comply with a requested restriction when: (i) the request concerns disclosures to a health plan for purposes of carrying out payment or health care operations and not for carrying out treatment; (ii) the disclosure is not otherwise required by law; and (iii) the PHI

pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket in full.

4. Any request for restrictions to the use of a patient's PHI must be approved by the Privacy Officer.

5. Should a request for restrictions be approved, Children's Dentistry of Amarillo is obligated to disclose or use PHI according to the terms of the accepted restrictions, unless otherwise excepted by HIPAA.

6. Any agreement to restrict the disclosure or use of PHI may be terminated for the following reasons:

   A. The individual requests or agrees to the termination in writing; or

   B. The Privacy Officer informs the patient in writing that Children's Dentistry of Amarillo is terminating the agreement to a restriction. A copy of the communication notifying the patient of the termination of the agreement to restrict use or disclosure of PHI will be maintained in the patient's medical record. Children's Dentistry of Amarillo may not unilaterally terminate a required agreement described in Number 3 above.

7. Children's Dentistry of Amarillo shall accommodate all reasonable requests for confidential communications and shall not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

8. Documentation of all requests for restrictions or for confidential communications as well as the approval or denial shall be documented and maintained in the individual's medical records.

Exhibit F1
Form

AUTHORIZATION TO RELEASE PROTECTED HEALTH INFORMATION

PATIENT NAME: _____ DATE: _____

PATIENT ADDRESS: _____ DOB: ___/___/___

_____

SOCIAL SECURITY #: _____-_____-_____

PATIENT'S TELEPHONE #: (_____) _____-_____

I hereby authorize _____
(***person/entity that has the protected health information, aka "Disclosing Entity"***)

and its employees and agents to release to:

_____
(***person, entity or class of persons to whom your protected health information may be provided***)

the following protected health information:

_____

_____
(***description of your protected health information to be used or disclosed by Disclosing Entity***)

for the purpose of:

_____

_____
(***description of each purpose of the requested use or disclosure or state "at the request of the individual"***)

I understand that the person or entity authorized to use or disclose my protected health information ("Disclosing Entity") under this Authorization to Release Protected Health Information will not condition treatment and coverage on me providing authorization. I understand that information used or disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and no longer be protected by federal regulations regarding privacy of health information. I also understand that I have the right to revoke this authorization at any time, except to the extent that the Disclosing Entity has taken action in reliance on the authorization, by delivering or sending written notice of revocation to the Disclosing Entity at the following address:

_____ _____

Name of Disclosing Entity **Phone Number**

_____

Street Address

_____

City/State/Zip Code

If I do not revoke this authorization, it will expire on _____

_____

(*expiration date or expiration event*)

_____ _____

Patient Signature **Date**

If the patient is unable to sign the authorization:

_____ by_ _____

Patient Name **Signor Signature and Date**

_____ _____

Relationship to Patient **Reason patient unable to sign and date authorization**

_____

Signor's Address (including city, state & zip code)

Signor's Phone Number: (_____) _____-_____

Exhibit F2
Policy and Procedure

POLICY TITLE: Privacy: Authorization	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI). In particular, the purpose of this policy is to ensure that Children's Dentistry of Amarillo obtains an authorization from a patient prior to disclosing the patient's PHI for purposes other than treatment, payment and health care operations or disclosures allowed by law.

POLICY

Unless otherwise allowed by law, Children's Dentistry of Amarillo will obtain an authorization from patients as required by HIPAA regulations for use or disclosure of PHI for specified purposes other than treatment, payment and health care operations or to disclose PHI to a third party specified by the patient.

SOURCE

45 C.F.R. § 164.508

PROCEDURE

Obtaining Authorization

1. An authorization is a customized document that gives Children's Dentistry of Amarillo permission to use specified PHI for a specified purpose.

2. An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization.

3. Children's Dentistry of Amarillo may not condition treatment or coverage on the patient providing authorization.

4. Unless approved by the Privacy Officer, Children's Dentistry of Amarillo may not release any PHI for purposes other than treatment, payment and health care operations without first obtaining a valid authorization.

5. Release of PHI for purposes other than treatment, payment and health care operations without a valid authorization or prior approval of the Privacy Officer will result in disciplinary action up to and including termination.

6. All requests for use or disclosure of PHI must be kept to the minimum necessary.[16] The minimum necessary requirement does not apply to disclosures to health care providers for treatment purposes.

7. A valid authorization must:

   A. Include a statement that the provider will not condition treatment or coverage on the patient providing authorization for the requested use or disclosure;

   B. Provide an expiration date or an expiration event (i.e. expires at the end of the patient's therapy, etc.);

   C. Be signed and dated by the patient or the patient's personal representative. If someone other than the patient signs the authorization for release of PHI, all required third party signor information must be indicated;

   D. Provide a specific and meaningful description of information to be used or disclosed and of each purpose of the requested use or disclosure or state that the authorization is "at the request of the individual."

   E. The authorization must specify the name or class of persons to whom Children's Dentistry of Amarillo may disclose the patient's PHI; or

   F. Specify the name or class of persons, or who may make disclosures to Children's Dentistry of Amarillo;

8. In the event that a patient transfers to another provider, Children's Dentistry of Amarillo may only release PHI to the new provider when:

   A. The new provider supplies Children's Dentistry of Amarillo with an authorization that includes the information detailed above;

---

[16] When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request (Final Standards for Privacy of Individually Identifiable Health Information § 164.502(b)).

B. The authorization must state that the new provider may request PHI from Children's Dentistry of Amarillo;

C. The authorization must specifically detail the purpose of the requested disclosure or use or state that the use or disclosure is at the request of the individual; and

D. The authorization must be signed and dated by the patient.

9. An authorization is considered invalid if:

A. It lacks any of the basic elements as set forth above;

B. The expiration date has passed;

C. Children's Dentistry of Amarillo knows the expiration event has occurred;

D. Children's Dentistry of Amarillo is aware that the authorization has been revoked;

E. Children's Dentistry of Amarillo knows that any information in the authorization is false; or

F. The authorization was combined with another document in violation of the Privacy Standards.

Patient Rights

1. The patient has a right to a copy of the signed and dated authorization.

2. The patient has the right to revoke authorization at any time except to the extent that Children's Dentistry of Amarillo has taken action relying on the authorization.

3. Any employee being notified by a patient either orally or in writing that the patient desires to revoke an authorization shall immediately notify the Privacy Officer.

Record Retention

Children's Dentistry of Amarillo must retain each signed authorization in the patient's medical record.

Exhibit G
Policy and Procedure

POLICY TITLE: Privacy: Disclosures of Protected Health Information without Authorization or Consent	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI) maintained by Children's Dentistry of Amarillo. In particular, the purpose of this policy is to ensure that a patient's PHI is not disclosed unless allowed by law.

POLICY

In accordance with the HIPAA regulations, Children's Dentistry of Amarillo may only release PHI for purpose other than treatment, payment and health care operations without authorization in accordance with HIPAA regulations.

SOURCE

45 C.F.R. §§ 164.506, 164.512

PROCEDURE

Children's Dentistry of Amarillo may release PHI for purposes other than treatment, payment and health care operations without authorization in the following situations:

1. Use or disclosure required by law including:
    A. Disclosures regarding victims of abuse;
    B. Disclosure for judicial and administrative proceedings; or
    C. Disclosure for law enforcement;
2. Use or disclosure for public health activities;

3. Use or disclosure for health oversight activities;

4. Use or disclosure about decedents;

5. Use or disclosure for cadaveric organs, eye or tissue donations;

6. Use or disclosure for research purposes;

7. Use or disclosure to avert serious threats to health or safety;

8. Use or disclosure for specialized government functions; and

9. Disclosure for Worker's Compensation.

In the instances listed above, a covered entity does not have to give the individual an opportunity to agree or object to the disclosure. Any disclosure without an authorization made pursuant to the reasons set forth above shall be approved in advance by the Privacy Officer.

Exhibit H
Policy and Procedure

POLICY TITLE: Privacy: Disclosures to Personal Representatives	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI). In particular, the purpose of this policy is to ensure the disclosure of PHI to a patient's personal representative is in accordance with HIPAA regulations.

POLICY

In accordance with the HIPAA regulations, Children's Dentistry of Amarillo may disclose PHI to a patient's personal representative.

SOURCE

45 C.F.R. § 164.502

PROCEDURE

Minors

1. A person may be considered a personal representative if under applicable law a person has the authority to act on behalf of an individual who is an adult or emancipated minor in making decisions related to health care.

2. An unemancipated minor has the authority to act as an individual with respect to PHI pertaining to a health service if:

    A. The minor assents to health care service; no other consent is required by law regardless of whether or not the consent of another has been obtained; and the minor has not requested that such person be treated as a personal representative;

B. The minor may lawfully obtain such health care service without the consent of another, and the minor, a court, or another person authorized by law has consented to such health care service; or

C. The parent, guardian, or other person acting in loco parentis agrees to an agreement of confidentiality between the covered entity and the minor.

3. In the case of an unemancipated minor who does not have authority to act on his or her own behalf, a parent, guardian, or other person acting in loco parentis who has authority under applicable law to act on behalf of the minor in making health care decisions and is considered a personal representative.

4. In cases where the individual who is the subject of the PHI is clearly an unemancipated minor and does not have the authority to act on his or her own behalf, PHI may be released to the parent or guardian of the minor child provided such release is in the best interest of the minor and in compliance with applicable law. However, if there is any doubt that the minor has authority to act on his or her own behalf or that the release may not be in the best interest of the child, the request for disclosure shall be referred to the Privacy Officer who shall make any determination related to such disclosure of PHI.

Disclosures to Personal Representatives

1. If a person is the personal representative of an individual, the person has the same rights and responsibilities as the individual. However, a covered entity may elect not to disclose PHI if the covered entity has a reasonable belief that:

   A. The individual may be subject to abuse or neglect; or

   B. Treating the person as the personal representative might endanger the individual and it is not in the best interest of the individual to treat the person as a personal representative.

2. Except as set forth above, any disclosure to a personal representative other than the parent of a minor child must be approved in advance by the Privacy Officer.

Exhibit I
Policy and Procedure

POLICY TITLE: Privacy: De-identifying PHI	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI) maintained by Children's Dentistry of Amarillo.

POLICY

Children's Dentistry of Amarillo will de-identify all PHI as required by HIPAA regulations.

SOURCE

45 C.F.R. § 164.514

PROCEDURE

1. PHI loses its HIPAA protections and can be freely disclosed if it does not identify an individual and there is no reasonable basis to believe that the information can be used to identify the patient.

2. Children's Dentistry of Amarillo will de-identify PHI when:

    A. Submitting information regarding a specific situation to obtain an opinion from a source that does not have a business associate agreement with Children's Dentistry of Amarillo;

    B. Submitting secondary claims with copies of Explanation of Benefits (EOB) that have multiple names on the EOB;

    C. Filing EOBs with multiple patient PHI into specific patient medical records; or

D. The disclosure is not otherwise authorized or allowed by law.

3. Information to be de-identified includes but is not limited to:

A. Patient name;

B. Health Insurance Claim number;

C. Policy number;

D. Social security number;

E. Medical record numbers;

F. All geographic subdivisions smaller than a state, including address, city, county, precinct and zip code;

G. Telephone numbers;

H. Fax numbers;

I. All elements of dates (except year) for dates directly related to a patient including:

i. Date of birth;

ii. Date of death;

iii. Admission date; and

iv. Discharge date.

J. E-mail address;

K. Web Universal Resource Locators (URLs);

L. Internet Protocol (IP) address numbers;

M. Full face photographic images;

N. Driver's license or other certificate numbers;

O. Vehicle license; and

P. Other patient specific identifiers.

Exhibit J
Policy and Procedure

POLICY TITLE: Privacy: Minimum Necessary	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI). In particular, the purpose of this policy is to ensure that Children's Dentistry of Amarillo complies with HIPAA requirements regarding releasing only the minimum amount of PHI necessary to accomplish the desired release.

POLICY

In accordance with the HIPAA regulations, Children's Dentistry of Amarillo will only release the minimum amount of PHI necessary to accomplish the purpose of the use, disclosure, or request for PHI.

SOURCE

45 C.F.R. §§ 164.502(b)(2), 164.502(e)

PROCEDURE

1. In accordance with HIPAA requirements, Children's Dentistry of Amarillo shall make reasonable efforts to ensure that a minimum amount of PHI is used or disclosed for any reason except for:

    A. Disclosures to or requests by a health care provider for treatment;

    B. Uses or disclosures made to the individual;

    C. Uses or disclosures made pursuant to an authorization;

    D. Disclosures made to the Secretary of HHS to investigate a privacy violation;

E. Uses or disclosures that are required by law; and

F. Uses or disclosures that are required for compliance with HIPAA.

2. Children's Dentistry of Amarillo must limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities. Any concerns regarding the release of the minimum necessary PHI should be directed to the Privacy Officer who will be responsible for determining what the minimum amount necessary is.

3. Children's Dentistry of Amarillo may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

4. Children's Dentistry of Amarillo shall restrict access to information by its employees to the minimum amount necessary for the employee to accomplish the employee's job functions.

5. Children's Dentistry of Amarillo may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

   A. Making disclosures to public officials if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

   B. The information is requested by another covered entity;

   C. The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

   D. Documentation or representations that comply with the applicable requirements of HIPAA have been provided by a person requesting the information for research purposes.

Exhibit K
Policy and Procedure

POLICY TITLE: Privacy: Marketing Disclosures	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI). In particular, the purpose of this policy is to ensure that a patient's PHI is not disclosed for marketing purposes unless such disclosure is in accordance with HIPAA regulations.

POLICY

In accordance with the HIPAA regulations, Children's Dentistry of Amarillo will not use or disclose PHI for marketing purposes without the prior approval of the Privacy Officer.

SOURCE

45 C.F.R. § 164.508(a)(3)

PROCEDURE

1. Children's Dentistry of Amarillo may not use or disclose PHI without an authorization for marketing purposes unless:

    A. The marketing communication:

        i. Occurs in a face-to-face encounter with the individual;

        ii. Concerns gifts or promotional items of nominal value; or

        iii. Concerns the health-related products and services of the covered entity or of a third party, is for treatment or health care operation purposes and the communication complies with HIPAA; and

B. Children's Dentistry of Amarillo does not receive direct or indirect payment from any party for making the communication.

2. Prior to using or disclosing the PHI of a patient for any marketing purposes, such use or disclosure must be approved in advance by the Privacy Officer.

Exhibit L1
Form

This sample Business Associate Agreement is intended only as a general guide. Any use of this Agreement should be reviewed by an attorney to ensure it is appropriate for the circumstances.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is made as of the ___ day of _____, 20__ ("Effective Date") by and between _____ ("Covered Entity") and _____ ("Business Associate").

BACKGROUND

Covered Entity and Business Associate wish to enter into this Agreement for purposes of complying with the Privacy, Security, Breach Notification, and Enforcement regulations at 45 CFR parts 160 and 164 (collectively the "HIPAA Standards"). The provisions of this Agreement apply with respect to all Protected Health Information ("PHI"), as defined in 45 CFR § 160.103, created, received, maintained, or transmitted by Business Associate in its representation of Covered Entity.

TERMS

In consideration of the mutual covenants contained herein, Business Associate and Covered Entity agree as follows:

1. Obligations of Business Associate.

(a) Business Associate will not use or disclose PHI other than as permitted or required by this Agreement or as required by law.

(b) Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the HIPAA Standards, and to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate will comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI.

(c) Business Associate will 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.

(d) To the extent the Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 CFR Part 164, Business Associate will comply with the requirements of 45 CFR Part 164, Subpart E that apply to Covered Entity in the performance of such obligations.

(e) Business Associate will report to Covered Entity (i) any use or disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware, and (ii) any security incident (as defined in 45 CFR § 164.304) of which it becomes aware. Business Associate will notify Covered Entity of any breach of unsecured PHI, as defined in 45 CFR § 164.402, without unreasonable delay and in no case later than five (5) calendar days after Business Associate discovers the breach.

(f) Business Associate will notify Covered Entity in writing promptly upon the discovery of any Breach of Unsecured PHI in accordance with the requirements set forth in 45 CFR §164.410, but in no case later than five (5) calendar days after discovery of a Breach. Business Associate will reimburse Covered Entity for any costs incurred by it in complying with the requirements of Subpart D of 45 CFR §164 that are imposed on Covered Entity as a result of a Breach committed by Business Associate.

(g) Business Associate will ensure that any agent, including a subcontractor, that receives PHI from Business Associate, or creates, receives, maintains, or transmits PHI on behalf of Business Associate, agrees to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such PHI and agrees to implement reasonable and appropriate safeguards to protect the security and privacy of such PHI, by entering into an agreement with such agent that meets the applicable requirements of the HIPAA Standards. If Business Associate enters into an agreement with any agent or subcontractor, Business Associate shall notify Covered Entity of the agreement within ten (10) calendar days and provide Covered Entity with a copy of such agreement.

(h) Business Associate will make books and records relating to the use and disclosure of PHI available to the Secretary of Health and Human Services ("Secretary") or the Secretary's designee, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the HIPAA Standards.

(h) At Covered Entity's request, Business Associate will make available PHI in Business Associate's possession to enable Covered Entity to respond to a request by an individual for access to PHI in accordance with 45 CFR § 164.524. In the event any Individual or personal representative requests access to the Individual's PHI directly from Business Associate, Business Associate shall immediately within five (5) business days, forward that request to Covered Entity. Any disclosure of, or decision not to disclose, the PHI requested by an Individual or a personal representative and compliance with the requirements applicable to an Individual's right to obtain access to PHI shall be the sole responsibility of Covered Entity.

(i) At Covered Entity's request, Business Associate will make available PHI in Business Associate's possession for amendment, and will incorporate any amendments to PHI, in accordance with 45 CFR § 164.526. In the event that any Individual requests that Business Associate amend such Individual's PHI or record in a Designated Record Set, Business Associate within five (5) business days will forward this request to Covered Entity. Any amendment of, or decision not to amend, the PHI or record as requested by an Individual and compliance with the requirements applicable to an Individual's right to request an amendment of PHI will be the sole responsibility of Covered Entity.

(j) Business Associate will maintain and will provide to Covered Entity upon request such documentation of disclosures of PHI 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 CFR § 164.528. In the event an Individual delivers the initial request for an accounting directly to Business Associate, Business Associate will within five (5) business days forward such request to Covered Entity. Business Associate will furnish to Covered Entity information collected in accordance with this request within five (5) business days after written request by Covered Entity, to permit Covered Entity to make an accounting of disclosures as required by 45 CFR §164.528, or in the event that Covered Entity elects to provide an Individual with a list of its business associates, Business Associate will provide an accounting of its disclosures of PHI upon request of the Individual, if and to the extent that such accounting is required under the HITECH Act or under HHS regulations adopted in connection with the HITECH Act.

2. Uses and Disclosures by Business Associate.

(a) Business Associate may use or disclose PHI to perform services for or on behalf of Covered Entity, provided that such use or disclosure would not violate the HIPAA Standards if made by Covered Entity.

(b) Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, if (i) the disclosure is required by law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it 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 person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Remedies for Breach. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity may either:

(a) 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;

(b) immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

(c) if neither termination nor cure is feasible, report the violation to the Secretary.

4. Term and Termination.

(a) This Agreement will be effective as of the Effective Date and will continue in effect until terminated. Either party may terminate this Agreement at any time, with or without cause, by giving thirty (30) days' written notice.

(b) Upon termination of this Agreement, for any reason, Business Associate will return or destroy all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity, if feasible. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate will 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 infeasible, for so long as Business Associate maintains such PHI.

5. Miscellaneous.

(a) Business Associate agrees to comply with all applicable state laws related to health information privacy. In the event state law is more stringent than a similar provision or requirement under the HIPAA Standards, Business Associate shall comply with such state law.

(b) Business Associate's data stewardship does not confer data ownership rights on Business Associate with respect to any data shared with it under the Agreement, including any and all forms thereof.

(c) This Agreement may not be assigned by either party without the prior written consent of the other party. Subject to the foregoing, this Agreement will be binding upon and will inure to the benefit of the parties and their respective successors and assigns.

(d) This Agreement may be amended only by written consent of the parties.

(e) Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever. There are no third-party beneficiaries to this Agreement.

(f) This Agreement constitutes the entire agreement between the parties concerning its subject matter
and supersedes all prior and contemporaneous agreements and understandings, express or implied, oral or written.

(g) This Agreement will be deemed to have been made in _____ and will be governed by and construed in accordance with _____ law. The section headings in this Agreement are for convenience only and will not affect its interpretation.

(h) This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which shall be deemed for all purposes to be one agreement. A facsimile or imaged signature shall be deemed an original signature for all purposes.

(i) Any notice or other communication by either party to the other will be in writing and will be deemed to have been given when hand delivered, sent by nationally-recognized overnight delivery service, or mailed, postage prepaid, registered or certified mail, addressed as follows:

If to Covered Entity: Name: _____
Address: _____
_____
Attn: _____

If to Business Associate: Name: _____
Address: _____
_____
Attn: _____

or to such other address as either party may designate by notice pursuant to this section.

IN WITNESS WHEREOF, Covered Entity and Business Associate have executed this Agreement effective as of the Effective Date.

[COVERED ENTITY]

By: _____
Name: _____
Title: _____

[BUSINESS ASSOCIATE]

By: _____
Name: _____
Title: _____

Exhibit L2
Form

This sample Business Associate Addendum is intended only as a general guide. Any use of this Agreement should be reviewed by an attorney to ensure it is appropriate for the circumstances.

BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum (the "Addendum") to the "[Name of Underlying Agreement"] (the "Agreement") between _____ ("Covered Entity") and Contractor, as defined under the Agreement, ("Business Associate") is incorporated into and made part of the Agreement for purposes of complying with the Privacy, Security, Breach Notification, and Enforcement regulations at 45 CFR parts 160 and 164 (collectively the "HIPAA Standards"). The provisions of this Addendum apply with respect to all Protected Health Information ("PHI"), as defined in 45 CFR § 164.501, created, received, maintained, or transmitted by Business Associate in its representation of Covered Entity.

TERMS

In consideration of the mutual covenants contained herein, Business Associate and Covered Entity agree as follows:

1. Obligations of Business Associate.

(a) Business Associate will not use or disclose PHI other than as permitted or required by this Addendum or as required by law.

(b) Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the HIPAA Standards, and to prevent use or disclosure of PHI other than as provided for by this Addendum. Business Associate will comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI.

(c) Business Associate will 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 Addendum.

(d) To the extent the Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 CFR Part 164, Business Associate will comply with the requirements of 45 CFR Part 164, Subpart E that apply to Covered Entity in the performance of such obligations.

(e) Business Associate will report to Covered Entity (i) any use or disclosure of PHI not provided for by this Addendum of which Business Associate becomes aware, and (ii) any security incident (as defined in 45 CFR § 164.304) of which it becomes aware. Business

Associate will notify Covered Entity of any breach of unsecured PHI, as defined in 45 CFR § 164.402, without unreasonable delay and in no case later than 10 calendar days after Business Associate discovers the breach.

(f) Business Associate will ensure that any agent, including a subcontractor, that receives PHI from Business Associate, or creates, receives, maintains, or transmits PHI on behalf of Business Associate, agrees to the same restrictions, conditions and requirements that apply to Business Associate with respect to such PHI, and agrees to implement reasonable and appropriate safeguards to protect the security and privacy of such PHI, by entering into an agreement with Business Associate that meets the applicable requirements of the HIPAA Standards.

(g) Business Associate will make books and records relating to the use and disclosure of PHI available to the Secretary of Health and Human Services ("Secretary") or the Secretary's designee, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the HIPAA Standards.

(h) At Covered Entity's request, Business Associate will make available PHI in Business Associate's possession to enable Covered Entity to respond to a request by an individual for access to PHI in accordance with 45 CFR § 164.524.

(i) At Covered Entity's request, Business Associate will make available PHI in Business Associate's possession for amendment, and will incorporate any amendments to PHI, in accordance with 42 CFR § 164.526.

(j) Business Associate will maintain and will provide to Covered Entity on request such documentation of disclosures of PHI 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 CFR § 164.528. Upon receipt of a request for an accounting directly from an individual, Business Associate will provide to the individual an accounting of disclosures made by Business Associate containing the information described in 42 CFR § 164.528.

2. Uses and Disclosures by Business Associate.

(a) Business Associate may use or disclose PHI to perform services for or on behalf of Covered Entity, provided that such use or disclosure would not violate the HIPAA Standards if made by Covered Entity.

(b) Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

(c) Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, if (i) the disclosure is required by law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it 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 person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Remedies for Breach. Upon Covered Entity's knowledge of a material breach of this Addendum by Business Associate, Covered Entity may either (i) provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Addendum if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; (ii) immediately terminate this Addendum if Business Associate has breached a material term of this Addendum and cure is not possible; or (iii) if neither termination nor cure is feasible, report the violation to the Secretary.

4. Return or Destruction of PHI Upon Termination. Upon termination of this Agreement, for any reason, Business Associate will return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, if feasible. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate will 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 infeasible, for so long as Business Associate maintains such PHI.

COVERED ENTITY: _____

By: _____
Name:
Title:

BUSINESS ASSOCIATE: _____

By: _____
Name: _____
Title: _____

Exhibit L3
Policy and Procedure

POLICY TITLE: Privacy: Business Associate Agreements	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and related Privacy Standards regarding the privacy of all protected health information (PHI). In particular, the purpose of this policy is to ensure that all business associates of Children's Dentistry of Amarillo provide it with adequate assurances that it will safeguard the PHI of Company's patients in accordance with the Privacy Standards.

POLICY

Children's Dentistry of Amarillo will obtain an approved Business Associate Agreement that meets the Privacy Standards' requirements for confidentiality prior to doing business with any entity that might have access to PHI while performing activities on behalf of Children's Dentistry of Amarillo.

SOURCE

45 C.F.R. §§ 160.103, 160.310

PROCEDURE

1. A business associate is any entity that Children's Dentistry of Amarillo contracts with in order to perform for on behalf of Children's Dentistry of Amarillo, health care activities and functions that involve use or disclosure of PHI, including but not limited to:

    A. Accounting firms;

    B. Independent consultants;

    C. Due diligence teams;

D. Lock boxes;

E. Legal counsel;

F. Software vendors;

G. Medical directors; and

H. Anyone else that requires PHI from Children's Dentistry of Amarillo in order to perform activities on behalf of Company.

2. In order for a business associate to carry out its functions, it is often necessary for Children's Dentistry of Amarillo to release PHI to that business associate.

3. Children's Dentistry of Amarillo will, in compliance with the Privacy Standards, obtain a Business Associate Agreement with that entity ensuring:

   A. The business associate will safeguard the PHI from misuse; and

   B. The business associate will help Children's Dentistry of Amarillo comply with regulations that provide patient's access to PHI about them and a history of disclosures.

4. Each Business Associate Agreement will contain all provisions required by the HIPAA regulations and will be implemented by the Privacy Officer.

5. A Business Associate Agreement must be signed by any potential business associates prior to releasing PHI to the business associate.

6. A new Business Associate Agreement is not required with each disclosure.

7. An agreement period may be indefinite or terminated, in writing, by either party.

8. The Privacy Officer will track all Business Associate Agreements including, but not limited to:

   A. Entity name;

   B. Address;

   C. Contract number;

   D. Time period of agreement; and

   E. Reason for accessing PHI.

9. A business associate may not utilize any PHI for its own use and:

   A. Must report to Children's Dentistry of Amarillo any uses or disclosures of PHI other than as stipulated in the Business Associate Agreement; and

   B. Return to Children's Dentistry of Amarillo or destroy (as applicable) all PHI at the end of the agreement period.

10. If Children's Dentistry of Amarillo becomes aware that a business associate has breached its obligation under the Business Associate Agreement, Children's Dentistry of Amarillo will:

   A. Take reasonable steps to cure the breach; or

   B. Terminate the business associate relationship.

11. The Privacy Officer will be notified immediately as soon as there is knowledge of such breach.

Exhibit M
Policy and Procedure

POLICY TITLE: Privacy: Breach Notification	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations under the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and related Privacy Standards regarding the privacy of all protected health information (PHI). In particular, the purpose of this policy is to ensure that Children's Dentistry of Amarillo makes the required notification when PHI has been breached.

POLICY

In accordance with HIPAA, HITECH, and related Privacy Standards, Children's Dentistry of Amarillo will make the required notification for any unauthorized breach of PHI, unless Children's Dentistry of Amarillo can demonstrate through a documented risk assessment that there is a low probability that PHI has been compromised.

SOURCE

45 C.F.R. §§§§ 164.402, 164.404, 164.406, 164.408

PROCEDURE

1. Breach notifications will be made without unreasonable delay and no more than 60 days after the discovery of the breach by Children's Dentistry of Amarillo or its business associates, unless otherwise directed by a law enforcement official.

2. Upon discovery of a breach by Children's Dentistry of Amarillo, Children's Dentistry of Amarillo will perform a documented risk assessment to determine if there is a low probability that PHI has been compromised. The risk assessment should, at a minimum, include an evaluation of the following factors:

A. The nature and extent of the PHI (e.g., sensitivity of the data, likelihood of re-identification);

B. The unauthorized person by whom/to whom the PHI was used/disclosed;

C. Whether the PHI was actually acquired or viewed; and

D. What actions have been taken to mitigate the impact of the unauthorized breach.

3. If it is determined that there is insufficient evidence to demonstrate that there is a low probability that the PHI has been compromised in an incident involving PHI under the control of either Children's Dentistry of Amarillo or its business associate, Children's Dentistry of Amarillo will make the notification as required by HITECH and related Privacy Standards. Such notice requirements are listed in 45 C.F.R. §§ 164.404, 164.406, and 164.408.

A. Actual written notice must be provided to the individual or individuals (or next of kin or personal representative, if applicable) affected by the breach.

B. If an individual or individuals cannot be reached via actual written notice, Children's Dentistry of Amarillo will provide substitute notice to the individual or individuals.

C. If Children's Dentistry of Amarillo determines imminent danger exists that the unsecured PHI will be misused, notification via telephone or other means will be made, in addition to the required actual written notice.

D. If over 500 individuals in one state or jurisdiction are affected by a breach, Children's Dentistry of Amarillo will provide written notice and notification to prominent media outlets in the state or jurisdiction where the affected individuals reside.

E. If over 500 individuals, regardless of location, are affected by a breach Children's Dentistry of Amarillo will make the required notification to the Secretary of the Department of Health and Human Services (Secretary) contemporaneously with the notice to individuals and no more than 60 days after the discovery of the breach.

F. If fewer than 500 individuals are affected by a breach, Children's Dentistry of Amarillo will document the breach in a log and submit the breach information annually to the Secretary, no more than 60 days after the end of the calendar year.

Exhibit N
Policy and Procedure

POLICY TITLE: Privacy: Violations	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with federal regulations created as the Health Insurance Portability and Accountability Act (HIPAA) regarding the privacy of all protected health information (PHI) maintained by Children's Dentistry of Amarillo. In particular, the purpose of this policy and procedure is to define the process for handling privacy complaints received from patients and/or workforce members.

POLICY

Children's Dentistry of Amarillo, through its Privacy Officer, will deal with all patient and/or workforce complaints regarding the privacy of PHI in a prompt and serious manner. All complaints will be addressed by the Privacy Officer in a manner consistent with the HIPAA regulations.

1. Privacy Officer will deal with all complaints in a timely manner. In most instances, this means that a response will be sent to the affected patient or employee no less than 30 days after receipt of the complaint from such patient or employee.

2. Privacy Officer will maintain active communication with the heads of any and all appropriate departments to verify that appropriate feedback is received regarding the effectiveness of the HIPAA compliance program and the availability of the complaint procedure to any patients and/or employees who wish to complain about the use or disclosure of PHI by Children's Dentistry of Amarillo.

3. Privacy Officer shall maintain files containing any and all complaints received by Children's Dentistry of Amarillo regarding the use or disclosure of PHI including documentation regarding the investigation and disposition of such complaint as well as any follow-up correspondence received from the patient and/or employee.

4. Violations of the Privacy Standards or the Security Standards by Children's Dentistry of Amarillo workforce members will result in discipline up to and including termination.

SOURCE

C.F.R. § 164.530

Exhibit O
Policy and Procedure

POLICY TITLE: Privacy and Security: Designation of Privacy and Security Officers	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with the Health Insurance Portability and Accountability Act (HIPAA), Children's Dentistry of Amarillo adopts this policy. In particular, the purpose of this policy and procedure is to guide the Children's Dentistry of Amarillo in designating Privacy and Security Officers responsible for implementing the Children's Dentistry of Amarillo's HIPAA compliance program.

POLICY

Children's Dentistry of Amarillo will assign the responsibility of implementing the HIPAA Compliance Program to an individual(s) familiar with HIPAA requirements and Children's Dentistry of Amarillo's services. The designated Privacy and Security Officers will be accountable to and will report to the Chief Executive Officer.

SOURCE

45 C.F.R. § 164.530

PROCEDURE

Designation of Privacy Officer

1. Children's Dentistry of Amarillo shall designate an individual to serve as Privacy Officer who will be responsible for the development and implementation of the privacy policies and procedures of the Company. Such designation will be documented and maintained in Children's Dentistry of Amarillo's records.

2. The individual designated as Privacy Officer must be responsible for and be able to fulfill, at a minimum, the following functions:

A. Being involved in the development of policies and procedures necessary for HIPAA compliance, in coordination with the entity's management and administration, privacy committee, and legal counsel;

B. Performing initial and periodic privacy risk assessments;

C. Ensuring that the Notice of Privacy Practices, Authorization, Acknowledgment, and other materials reflecting the entity's privacy practices are compliant with HIPAA;

D. Ensuring delivery of initial and periodic privacy training to all employees, medical and professional staff, contractors, and other appropriate third parties;

E. Reviewing all contracts with business associates to ensure that HIPAA requirements are being met;

F. Establishing mechanisms to track access to PHI;

G. Being responsible for ensuring the entity does not infringe upon an individual's right to inspect, amend, and restrict access to PHI when appropriate;

H. Establishing and administering a process for receiving, documenting, tracking, investigating, and responding to all complaints concerning the entity's privacy policies and procedures;

I. Ensuring compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the entity's workforce;

J. Being aware of applicable federal and state privacy laws and accreditation standards;

K. Cooperating with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations; and

L. Working with Children's Dentistry of Amarillo's administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) that undertake to adopt or amend privacy legislation, regulation or standard.

Designation of Security Officer

1. Children's Dentistry of Amarillo will appoint an individual who has full understanding of its services and IT systems to serve as the Security Officer.

2. Children's Dentistry of Amarillo may assign the duty of Security Officer to the same individual who serves as Chief Information Officer of the IT Department or may determine that the Privacy Officer should also serve as the Security Officer.

3. The individual designated as the Security Officer must be responsible for and able to fulfill the following functions as a minimum:

   A. Serving as the point of contact for the HIPAA Security Compliance Program;

   B. Overseeing development and maintenance of HIPAA Security Policies and Procedures;

   C. Managing implementation of the HIPAA Security Policies and Procedures and ensuring adherence to such policies and procedures;

   D. Communicating the HIPAA Security Policies and Procedures to the workforce;

   E. Administering the risk analysis;

   F. Working with technical personnel to ensure an integrated and thorough program that protects electronic PHI;

   G. Participate in determining IT security investments and purchases;

   H. Ensuring that the security risks are investigated and addressed;

   I. Receiving, documenting, and responding to complaints and inquiries about security matters; and

   J. Implementing periodic security evaluations and responding to such evaluations.

Exhibit P
Policy and Procedure

POLICY TITLE: Security: Risk Analysis	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

To ensure compliance by Children's Dentistry of Amarillo with the Health Insurance Portability and Accountability Act (HIPAA) and related Security Standards regarding the security and integrity of all electronic protected health information (EPHI) maintained by Children's Dentistry of Amarillo, Children's Dentistry of Amarillo adopts this policy. In particular, the purpose of this policy and procedure is to determine Children's Dentistry of Amarillo's weaknesses that leave EPHI vulnerable to improper use or disclosures and implement security measures sufficient to reduce risks.

POLICY

In accordance with HIPAA, HITECH, and related Security Standards, Children's Dentistry of Amarillo will follow risk assessment procedures, periodically, and implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

SOURCE

45 C.F.R. §§ 164.306(b) - 164.306(e)

PROCEDURE

1. Children's Dentistry of Amarillo will identify weaknesses that leave EPHI vulnerable to improper use or disclosure and will implement security measures sufficient to reduce identified risks. Children's Dentistry of Amarillo may use questionnaires, conduct on-site interviews, review documents, or utilize automated scanning tools to gather information necessary for the risk analysis.

2. On a periodic basis, Children's Dentistry of Amarillo will take the following steps to conduct the risk assessment and to address identified risks:

A. Inventory the locations, devices, and information technology (IT) systems that have access to EPHI.

B. Establish, review and update protocols that prevent unauthorized alteration, ensure confidentiality, and protect availability of EPHI at each location, device, and system. Children's Dentistry of Amarillo will further determine whether the established protocols satisfy the standards set forth in Security Standards. A checklist of the standards is included in Children's Dentistry of Amarillo's HIPAA Manual.

C. For each location, device, and system, identify the weaknesses that pose a risk to the integrity, confidentiality, and availability of EPHI. Children's Dentistry of Amarillo will consider the likelihood of human threats (such as fires, earthquakes, and floods); and environmental failures (such as power outages and liquid leakages).

D. Depending on (i) the impact on EPHI if the weakness was exploited and (ii) the likelihood that the recognized threat will occur, label the risk as high, medium, or low.

E. Document the results of the assessment.

F. Designate an individual to review and approve the results of the assessment. The designated individual should be independent of the personnel conducting the risk assessment.

G. Ascertain measures needed to comply with the Security Standards and reduce the risks identified in the risk analysis, prioritizing from high to medium to low.

H. Document the measures adopted in response to the risk analysis.

Exhibit Q
Policy and Procedure

POLICY TITLE: Privacy and Security: Sanctions	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Security Standards regarding the security and integrity of all electronic protected health information (EPHI) maintained by Children's Dentistry of Amarillo. In particular, the purpose of this policy and procedure is to establish sanctions against workforce members who fail to comply with the security policies and procedures.

POLICY

Children's Dentistry of Amarillo will implement appropriate, fair, and consistent sanctions for workforce members who fail to comply with the privacy and/or security policies and procedures of Children's Dentistry of Amarillo.

1. Children's Dentistry of Amarillo will identify violations of its HIPAA compliance program as grounds for sanctions against workforce members in any document that outlines Children's Dentistry of Amarillo's right to take such action.

2. Children's Dentistry of Amarillo will ensure that the sanction (e.g., reprimand, termination, etc.) varies depending on the severity of the violation and that sanctions will apply equally to all members of the workforce.

3. Children's Dentistry of Amarillo will provide proper notice to the workforce by requiring workforce members to sign a form acknowledging Children's Dentistry of Amarillo's security measures and the sanctions for non-compliance.

4. Children's Dentistry of Amarillo will document sanctions that are applied, if any.

SOURCE

45 C.F.R. § 164.308(a)(1)(ii)(C)

Exhibit R
Policy and Procedure

POLICY TITLE: Privacy and Security: Training and Security Awareness	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Privacy and Security Standards regarding the privacy, security and integrity of all protected health information (PHI) maintained by Children's Dentistry of Amarillo. In particular, the purpose of this policy and procedure is to implement a privacy and security awareness and training program for workforce members who have access to PHI to help reduce the likelihood of breaches and HIPAA violations.

POLICY

Children's Dentistry of Amarillo will develop and implement a privacy and security awareness and training program to inform its workforce members of anticipated security risks and appropriate responses.

SOURCE

45 C.F.R. § 164.308(a)(5)(i); Tex. Health & Safety Code § 181.101

PROCEDURE

Training

1. Children's Dentistry of Amarillo must train all of its workforce on the policies and procedures with respect to PHI and EPHI as necessary and appropriate for the members of the workforce to carry out their respective responsibilities.

2. As part of required training, all workforce members will be instructed on:

    A. Protection against malicious software, including how to guard against, detect and report malicious software;

B. Log-in monitoring and reporting any discrepancies to the Security Officer;

C. Password management; and

D. Potential vulnerabilities regarding workforce members' remote access.

3. Required training must be provided to each member of the workforce:

A. No later than the 90th day after the date a new employee is hired; and

B. Within a reasonable period of time after any material change in the privacy and/or security policies and procedures that affects the member's functions, but not later than the first anniversary of the date the material change takes effect; and

4. Each member who receives training must sign, electronically or in writing, a statement verifying the member's completion of training and the Security Officer will document all activities and efforts related to security awareness and training. Such documentation shall be retained for six (6) years after the training date.

Security Program

1. Children's Dentistry of Amarillo must have a program that informs the organization and its workforce members of anticipated security risks to electronic PHI and appropriate responses. The program must include the following features:

A. Protection from Malicious Software. The program must include features for guarding against, detecting, and reporting malicious software. All equipment (computers, laptops, smart phones, portable devices, etc.) that maintain, transmit, receive, or access EPHI will have software that detects, reports, and protects against malicious software.

i. The Security Officer will be responsible for the selection of malware protection programs and procedures to ensure that the most powerful and appropriate techniques and methods are used to protect Children's Dentistry of Amarillo's information systems and the EPHI they contain.

ii. The personnel responsible for IT will install and regularly update firewall and virus protection software on all devices, servers, and other systems that maintain, transmit, receive, or access EPHI.

iii. Each workforce member will be instructed to promptly report any suspected malicious software and will take precautions not to

introduce any malicious software into Children's Dentistry of Amarillo's computer systems.

B. Log-in Monitoring. The Security Officer must designate an individual to be responsible for monitoring log-in attempts to any device or system that maintains, transmits or provides access to EPHI. The monitoring program shall include a feature that generates reports regarding discrepancies or questionable or illegal conduct. The Security Officer will routinely review and investigate as needed any reports generated by the program.

C. Password Management. The program must include features for creating, changing, and safeguarding passwords so that such passwords remain secure and confidential.

i. All workforce members must utilize strong passwords and pass-phrases.

ii. All passwords or pass-phrases used to access systems containing, transmitting, receiving, or using EPHI must be a minimum of eight (8) characters and should include non-alphanumeric characters or symbols.

iii. Workforce members are prohibited from writing down any passwords or pass-phrases and keeping them at workstations or near computers.

iv. All workforce members will change their passwords or pass-phrases at least every ninety (90) days.

v. The Security Officer will determine whether some or all workforce members' passwords or pass-phrases need to be changed in the event an information system is compromised.

vi. Passwords or pass-phrases must be changed immediately if they are suspected of being disclosed or shared with another user or unauthorized person.

vii. The Security Officer will be immediately notified if a workforce member forgets or experiences any compromise of their password or pass-phrase.

viii. Children's Dentistry of Amarillo's training and security program will emphasize proper password management.

2. The Security Officer will ensure that the workforce has access to Children's Dentistry of Amarillo's current security policies and procedures. Furthermore, the

Security Officer will periodically distribute emails or memoranda addressing topics relevant to Children's Dentistry of Amarillo's needs and explaining noteworthy security policies.

Exhibit S
Policy and Procedure

POLICY TITLE: Security: Information System Activity Review and Security Incidents	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Security Standards regarding the security and integrity of all electronic protected health information (EPHI). In particular, the purpose of this policy and procedure is to establish and manage any information systems activity review process and outline procedures to respond to and address security incidents involving EPHI.

POLICY

Children's Dentistry of Amarillo will implement procedures to regularly review records of information system activity and implement audit and review functions. Children's Dentistry of Amarillo will also implement policies and procedures to identify and appropriately respond to security incidents involving EPHI.

SOURCE

45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312

PROCEDURE

Information System Activity Review

1. Children's Dentistry of Amarillo must have an IT system that tracks access and use of EPHI and that can alert Children's Dentistry of Amarillo to any successful or attempted unauthorized access, use, disclosure, modification or destruction of EPHI ("Security Incident").

2. The Security Officer will review periodically and revise as necessary the following aspects of IT system and auditing features: (i) the third-part(ies), operating system(s) or software program(s) that track and audit attempted and successful

access and use of EPHI; (ii) the activities (e.g., access to, creation of, editing, and/or deletion of EPHI) tracked and audited by such parties, systems, or programs; and (iii) information included on the audit reports.

3. The Security Officer will audit logs and access reports generated by the IT system as well as all Security Incident tracking reports. The Security Officer will assess such information and respond appropriately in order to prevent, detect, contain, and correct security violations.

4. All information system activity reviews will be documented and retained to ensure HIPAA compliance.

Tracking and Responding to Security Incidents

1. Security Incidents include attempted and successful unauthorized access to or use, disclosure, modification, or destruction of EPHI and interference with operations of information systems.

2. The Security Officer will take the following steps to detect and appropriately respond to a security incident:

   A. Monitor alerts from antivirus software, watch for the appearance of filenames with unusual characters in the system, and monitor failed log-in attempts.

   B. Develop a reporting template so that the workforce may report any security incidents, such as loss or exposure of EPHI.

   C. When a suspected Security Incident is reported to the Security Officer, the Security Officer will:

      i. Rapidly identify and classify the severity of the Security Incident and inventory the systems and information affected by the incident;

      ii. Determine the actual risk to EPHI;

      iii. Identify the source of the incident and repair, patch, or otherwise correct the condition or error that created the Security Incident;

      iv. Retrieve or limit dissemination of EPHI, if possible; and

      v. If the incident was successful, investigate why existing protective measures did not prevent it.

D. If PHI or EPHI was involved in the Security Incident, the Security Officer will be responsible for determining whether the Security Incident is also a Breach of Unsecured PHI.

E. The Security Officer is responsible for mitigating the harmful effects of any Security Incident and for implementing appropriate sanctions in response to the incident.

F. Each Security Incident must be fully documented, including each step taken in the investigation and response process.

Exhibit T
Policy and Procedure

POLICY TITLE: Security: Workforce Access to EPHI	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Security Standards regarding the security and integrity of all electronic protected health information (EPHI). In particular, the purpose of this policy and procedure is to ensure that all members of the workforce have appropriate access to EPHI, and to prevent those workforce members who do not have such access from obtaining access to EPHI.

POLICY

Children's Dentistry of Amarillo will develop methods to supervise locations and systems where EPHI is available, and authorize each workforce member's access to EPHI to ensure that members of the workforce have a level of access appropriate to their responsibilities. Children's Dentistry of Amarillo will also adopt procedures to terminate workforce members' access.

SOURCE

45 C.F.R. §§ 164.308, 164.312

PROCEDURE

1. The Human Resources (HR) Department and IT Department will collaborate to ensure that workforce members and business associates have the minimum necessary authorization rights and that such rights are terminated when appropriate. HR will promptly inform the IT Department of workforce members and business associates requiring access to EPHI. HR will also promptly inform the IT Department of any current or former workforce members or business associates whose access should be terminated. The IT Department will grant and terminate access to EPHI and maintain an updated log of access rights assigned to each employee and business associate.

2. Access to EPHI will be granted to a new workforce member after the individual receives training on EPHI. The individual will receive access to EPHI to the extent appropriate for his or her job and will be limited to the minimum necessary to accomplish his or her workforce tasks. An individual is prohibited from attempting to exceed their level of authorized access.

3. An individual's access to EPHI must be terminated when the person is no longer a workforce member; when access is no longer appropriate for the individual's role in the workforce; or when the individual has been sanctioned for serious offenses or violations of these HIPAA Privacy or Security Policies and Procedures.

4. Personnel involved in or aware of the termination of a workforce member shall promptly notify the IT Department and HR.

    A. The IT Department will identify and terminate any electronic access rights previously granted to the individual. Such actions will be documented.

    B. HR will identify all ID badges, access cards, keys, and other such items that enabled the person to access PHI and EPHI. HR will retrieve, inventory, and document all such items.

5. Computer and system access control is achieved by requiring workforce members authorized to access EPHI to have unique user IDs and unique passwords.

6. All workforce members who have access to EPHI will be appropriately supervised through periodic monitoring of their use of information technology systems.

7. The Security Officer will review access rights to PHI and EPHI systems on an annual basis and every time a workforce member's employment status changes, the Security Officer will determine whether access rights should be granted, modified, or revoked.

Exhibit U
Policy and Procedure

POLICY TITLE: Security: Facility Access Controls; Workstation Use and Security; and Media Controls	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Security Standards regarding the security and integrity of all electronic protected health information (EPHI). In particular, the purpose of this policy and procedure is to implement policies and procedures that address the physical safeguards and arrangement of workspace and technological systems.

POLICY

Children's Dentistry of Amarillo will implement policies and procedures that limit physical access to its electronic information systems; specify the proper functions to be performed and the physical attributes of a specific workstation that can access EPHI; and restrict access of EPHI to authorized users. Children's Dentistry of Amarillo will also implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI.

SOURCE

45 C.F.R. §§ 164.308, 164.312

PROCEDURE

Facility Access Controls

1. Children's Dentistry of Amarillo will take the following steps to limit physical access to its electronic information systems and the facility in which they are housed:

    A. Inventory all physical spaces where one could access EPHI, including technology devices located in the physical space and employees with remote access privileges.

B. Establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

C. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

D. Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

E. Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks).

Workstation Use and Security

1. Children's Dentistry of Amarillo will develop and implement workstation use and security procedures associated with specific functions, procedures, and appropriate environments of workstations that access EPHI. Such procedures will include:

   A. Determining the scope of allowable use for each computing device.

   B. Tagging electronic equipment so that any lost or stolen device may be tracked back to Children's Dentistry of Amarillo.

   C. Arranging devices in such a manner that unauthorized persons cannot view any displays of EPHI.

   D. Employing locking mechanisms to further protect portable devices.

   E. To the extent that any workforce member works remotely, the same security restrictions shall apply to the remote workstation.

Device and Media Controls

1. Children's Dentistry of Amarillo will develop policies and procedures for the proper use of memory devices that are either transportable from or attached to electronic computing devices, such as discs, memory sticks, and hard drives.

2. Children's Dentistry of Amarillo will implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.

3. Children's Dentistry of Amarillo will implement procedures for removal of EPHI from electronic media before the media are made available for re-use. Such procedures include:

   A. Removal of all EPHI from memory devices when the devices are either recycled or destroyed.

   B. Delegation of removal and/or deletion responsibility to appropriate personnel and ensure documentation of the activity.

4. Maintain a record of the movements of hardware and electronic media and any person responsible therefor. Such procedures will include:

   A. Limiting employees' rights to use transportable memory devices; and

   B. For employees who have the right to store EPHI on memory devices, purchasing and assigning devices to employees and keeping an inventory of the memory devices and their assigned use.

5. Create a retrievable, exact copy of EPHI, when needed, before movement of equipment.

Exhibit V
Policy and Procedure

POLICY TITLE: Security: Contingency Plan	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Security Standards regarding the security and integrity of all electronic protected health information (EPHI). In particular, the purpose of this policy and procedure is to establish written protocols that identify how to respond in an emergency situation.

POLICY

The Security Officer along with other appropriate personnel will establish a contingency plan for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI by implementing emergency preparedness, data backup and disaster recovery plans and test and revise procedures for such plans.

SOURCE

45 C.F.R. § 164.312

PROCEDURE

Emergency Preparedness Plan

1. The Security Officer will establish procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.

2. Children's Dentistry of Amarillo will use the Emergency Preparedness Plan when operating in "emergency mode."

3. "Emergency mode" will be triggered by one or more of the following occurrences:

A. Electrical power is unavailable for more than eight (8) consecutive hours;

B. A fire, flood, storm, natural disaster or other occurrence hinders normal business operations for more than twenty-four (24) consecutive hours.

4. The Security Officer will document all emergency planning and preparedness activities.

Data Backup Plan

1. The Security Officer will establish a procedure to create and maintain retrievable and identical copies of EPHI, at a separate offsite location or otherwise, to timely respond to an unexpected event or emergency (e.g., fire, flood, outages, natural disasters, viruses, hackers, etc.) and resume its normal business operations.

2. The Security Officer will perform regular backups on the network, including shared drives containing EPHI, application and financial data, and crucial system information.

   A. Data will be automatically backed up on a daily, or otherwise regular basis.

3. The Security Officer will validate the accuracy, integrity, and completeness of the backup performed from the previous night by using available reporting utilities.

   A. The Security Officer will generate a data backup report which will be maintained for a period not less than thirty (30) days and the report will be logged in the network log.

   B. The Security Officer will immediately take action if any errors in the backup data occur.

   C. The Security Officer will replace backup media in accordance with the manufacturer's recommended guidelines.

4. The Security Officer will quarterly test the validity of backup data and the ability to restore data in the event of a computer system failure or occurrence of disaster.

5. The Security Officer will log successful restore functions in the network log and will take immediate action on any problems identified during the restore function no later than the same business day that they occur. Designated personnel will use contracted technical support/vendors as needed to resolve problems and ensure the validity of backup data.

6. All personnel who detect or suspect a data backup problem shall report it to the Security Officer and designated personnel will follow up with a written memorandum that includes:

A. A narrative of the data backup problem;

B. The length of time the problem has existed; and

C. Suggested solutions to the problem.

Disaster Recovery Plan

1. Children's Dentistry of Amarillo will maintain planning procedures such that in the event of an unexpected negative occurrence, Children's Dentistry of Amarillo will be able to maintain normal business operations with as little disruption as possible.

2. All workforce members shall take the following steps related to recovering PHI and EPHI:

   A. Properly back up computerized files in accordance with this policy;

   B. Ensure that media is stored properly;

   C. Protect all servers and other critical equipment from damage in the event of an electrical outage by using uninterruptible power supplies; and

   D. Receive training in disaster preparation and recovery.

3. The Security Officer will take the following steps related to recovering PHI and EPHI:

   A. Ensure that major hardware is covered under property and casualty insurance or other insurance policies;

   B. Periodically check that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly and ensure that workforce members are trained in their use.

4. The Security Officer or an appropriate third-party vendor will prepare, analyze, test, and update plans for contingency operations on a periodic basis to ensure the restoration of lost data in the event of an emergency.

   A. Contingency operations will be activated during or immediately following an emergency or disaster situation. The Security Officer may designate personnel to have access to facilities and systems to restore lost data even if Children's Dentistry of Amarillo is not otherwise accessible.

Test and Revisions Procedures for Contingency Plans.

1. Children's Dentistry of Amarillo will periodically test and revise, if needed, all emergency preparedness plans, including emergency and contingency plans in this policy.

2. The Security Officer will ensure that all such plans are up-to-date and meet emergency preparedness requirements. The Security Officer will review such plans and revise as necessary on an annual basis, and copies of all plans will remain on file and be available to all personnel.

    A. Workforce members will also evaluate the emergency and contingency plans on an annual basis using a scenario-based walk-through.

3. The Security Official will periodically conduct technical and nontechnical evaluations of the emergency and contingency plans.

Exhibit W1
Policy and Procedure

POLICY TITLE: Security: Annual Evaluation of HIPAA Security Compliance Program	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Security Standards regarding the security and integrity of all electronic protected health information (EPHI). In particular, the purpose of this policy and procedure is to establish an annual evaluation of the effectiveness of the security program.

POLICY

The Security Officer will perform an annual technical and nontechnical evaluation, based upon Security Standards under HIPAA and, subsequently, in response to environmental or operational changes affecting the security of EPHI.

SOURCE

45 C.F.R. § 164.316

PROCEDURE

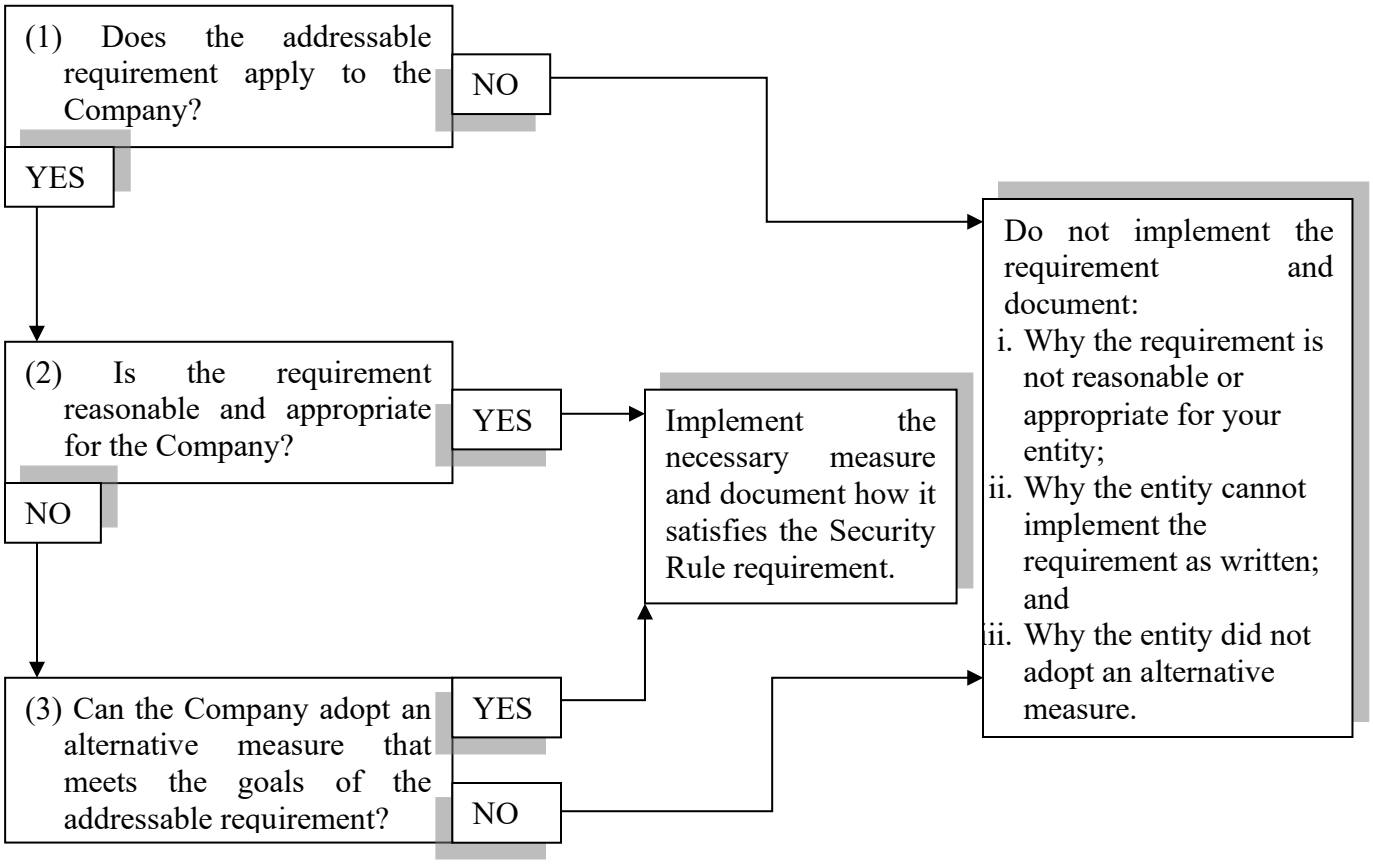
1. The Security Officer will address both technical safeguards, such as firewalls and anti-virus software as well as non-technical procedures (e.g., the workforce training program) in its annual evaluation.

2. The attachments to this policy will be used to the guide the Security Officer's evaluations of the Security Program.

3. The Security Officer will conduct additional evaluations when the officer determines that changes in business operations may affect the safety of EPHI.

Exhibit W2
Annual Evaluation
Addressable Standards

The Security Rule labels certain requirements as "addressable." Children's Dentistry of Amarillo ("Practice") will implement policies and procedures in accordance with addressable requirements unless a particular requirement is neither reasonable nor appropriate for the entity. Practice will use the following question tree to assess and comply with addressable requirements included in 45 C.F.R. Part 164, Subpart C.



SOURCE

45 C.F.R. § 164.316

Exhibit W3
Annual Evaluation
Security Standards Checklist

The Security Rule requires Children's Dentistry of Amarillo ("Practice") to adopt policies and procedures that implement the requirements identified in the first column of the below table. Practice will periodically review its policies and procedures and determine whether Practice's security program satisfies the legal requirements in the first column. Practice will utilize the following table or a comparable to document to record how the Practice's security program complies with each Security Rule requirement.

Standards	Sections of 45 C.F.R.	Implementation Specifications (R) = Required, (A) = Addressable	Yes / No	Details on the entity's adopted procedures
Administrative Safeguards				
Security Management Process	164.308(a)(1)	Risk Analysis (R)		
		Risk Management (R)		
		Sanction Policy (R)		
		Information System Activity Review (R)		
Assigned Security Responsibility	164.308(a)(2)	(R)		
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)		
		Workforce Clearance Procedure		
		Termination Procedures (A)		
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)		

Standards	Sections of 45 C.F.R.	Implementation Specifications (R) = Required, (A) = Addressable	Yes / No	Details on the entity's adopted procedures
		Access Authorization (A)		
		Access Establishment and Modification (A)		
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)		
		Protection from Malicious Software (A)		
		Log-in Monitoring (A)		
		Password Management (A)		
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)		
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)		
		Disaster Recovery Plan (R)		
		Emergency Mode Operation Plan (R)		
		Testing and Revision Procedure (A)		
		Applications and Data Criticality Analysis (A)		
Evaluation	164.308(a)(8)	(R)		
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)		
Physical Safeguards				

Standards	Sections of 45 C.F.R.	Implementation Specifications (R) = Required, (A) = Addressable	Yes / No	Details on the entity's adopted procedures
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)		
		Facility Security Plan (A)		
		Access Control and Validation Procedures (A)		
		Maintenance Records (A)		
Workstation Use	164.310(b)	(R)		
Workstation Security	164.310(c)	(R)		
Device and Media Controls	164.310(d)(1)	Disposal (R)		
		Media Re-use (R)		
		Accountability (A)		
		Data Backup and Storage (A)		
Technical Safeguards (see §164.312)				
Access Control	164.312(a)(1)	Unique User Identification (R)		
		Emergency Access Procedure (R)		
		Automatic Logoff (A)		
		Encryption and Decryption (A)		
Audit Controls	164.312(b)	(R)		

Standards	Sections of 45 C.F.R.	Implementation Specifications (R) = Required, (A) = Addressable	Yes / No	Details on the entity's adopted procedures
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)		
Person or Entity Authentication	164.312(d)	(R)		
Transmission Security	164.312(e)(1)	Integrity Controls (A)		
		Encryption (A)		

Exhibit X
Policy and Procedure

POLICY TITLE: Security: Technical Safeguards	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Security Standards regarding the security and integrity of all electronic protected health information (EPHI). In particular, the purpose of this policy and procedure is to implement practices and technology operations to ensure that only authorized personnel and software programs access EPHI.

POLICY

Children's Dentistry of Amarillo will implement technology that will protect the authenticity of EPHI and secure information during transmission as well as regulate access to and audit the use of EPHI.

SOURCE

45 C.F.R. §§ 164.308, 164.312

PROCEDURE

Access Controls

1. Children's Dentistry of Amarillo will implement technical policies and procedures to allow EPHI access only to those persons or software programs that have been granted specific rights.

2. Children's Dentistry of Amarillo will assign a unique name/user ID for identifying and tracking user identity for each member of the workforce who has access to EPHI.

A. All workforce members shall promptly report any lost User ID's immediately to the Security Officer.

3. For systems in which the security of EPHI is at risk, Children's Dentistry of Amarillo will implement two-level or multi-factor authentication, such as password authentication plus a security question and associated procedures for authentication.

   A. Company will limit authentication attempts to its EPHI attempts to its device access. The Security Officer will determine the limit for access attempts. Authentication attempts that exceed the limit may result in:

      i. Disabling the relevant account for an appropriate period of time; or

      ii. Logging of the event.

   B. All workforce members must change their password periodically.

   C. All workforce members must promptly report any lost passwords immediately to the Security Officer.

4. Children's Dentistry of Amarillo will implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

   A. After a period of fifteen (15) minutes of inactivity, or other appropriate amount of time specified by the Security Officer, a user will automatically be logged off of the information system and all workstations will be configured such that a password protected screen saver is automatically activated.

   B. The Security Officer will develop and implement such automatic log-off and screen saver functions.

5. Children's Dentistry of Amarillo will implement a mechanism to encrypt and decrypt EPHI.

   A. The Security Officer will develop and implement specific encryption and decryption functions and procedures. These procedures will specify the appropriate use and application of encryption and decryption for all computers, mobile devices, and workstations that access EPHI.

   B. Encryption will be used to:

      i. Protect all cryptographic keys against modification and destruction;

ii. Protect private keys against authorized disclosure;

iii. Implement a documented process for managing the cryptographic keys used to encrypt EPHI which is stored or maintained on Company's information system; and

iv. Determine activation and deactivation dates for its cryptographic keys periodically.

C. Encryption solutions include secure socket layer (SSL) and hypertext transfer protocol secure (HTTPS).

6. Children's Dentistry of Amarillo will implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

7. The Security Officer will document all activities taken in accordance with this policy and procedure.

Integrity Controls

1. Children's Dentistry of Amarillo must ensure the authenticity of EPHI both while it is stored and when it is transmitted. To comply with this standard, Children's Dentistry of Amarillo will:

A. Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.

B. Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.

C. Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

D. Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.

E. Implement a mechanism to encrypt EPHI.

Audit Controls

1. Children's Dentistry of Amarillo will establish and maintain audit controls, and the Security Officer will be responsible for the development and implementation of audit controls and associated procedures.

2. Workforce members must cooperate with any audit by providing access to all information systems used, regardless of location.

3. Audit controls may be utilized remotely with or without the workforce member's knowledge.

4. Audit controls and functions will log the date, time, user, and recipient of any disclosed EPHI. Audit logs may track additional information.

Exhibit Y
Policy and Procedure

POLICY TITLE: Privacy Rule: Use and Disclosure of Mental Health Records	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Privacy Standards. In particular, the purpose of this policy and procedure is to ensure compliance with HIPAA requirements regarding the use and disclosure of a patient's mental health records.

POLICY

Children's Dentistry of Amarillo will comply with the requirements for the use and disclosure of PHI relating to a patient's mental health records and psychotherapy notes.

SOURCE

45 C.F.R. § 164.508

PROCEDURE

1. Generally, the HIPAA Privacy Rule applies uniformly to all PHI, without regard to the type of information. Therefore, Children's Dentistry of Amarillo must comply with all aspects of the HIPAA Privacy Rule outlined in the HIPAA Manual as applied to all PHI, including mental health records. Psychotherapy notes are treated differently than other types of PHI, however. Greater restrictions are placed on the use and disclosure of such notes.

2. Psychotherapy notes are notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session that are separated from the rest of the individual's medical records. Psychotherapy notes do not include any information that is maintained in a patient's medical record.

3. Children's Dentistry of Amarillo must obtain authorization for any use or disclosure of psychotherapy notes for any reason, except for the following uses or disclosures. Such uses and disclosures will be made in compliance with the minimum necessary rule and the regulations set forth in 45 C.F.R. § 164.508(a)(2). Children's Dentistry of Amarillo may use or disclose psychotherapy notes without first obtaining an authorization:

   A. To carry out the following treatment, payment or health care operations:

      i. Use by the originator of the psychotherapy notes for treatment;

      ii. Use or disclosure by Children's Dentistry of Amarillo for its own training programs; and

      iii. Use or disclosure by Children's Dentistry of Amarillo to defend itself in a legal action or other proceeding brought by the individual.

   B. To make disclosures in the following situations:

      i. Disclosure required by the Office for Civil Rights to determine compliance with HIPAA;

      ii. Disclosures that Children's Dentistry of Amarillo is permitted to make to the individual's personal representative;

      iii. Disclosures to a health oversight agency for oversight activities relating to the originator of the psychotherapy notes;

      iv. Disclosures to a coroner or medical examiner for purposes of identifying a deceased person, determining a cause of death, or other duties as authorized by law; and

      v. Disclosure based on a good faith belief that such disclosure is necessary (i) to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; (ii) for law enforcement authorities to identify or apprehend an individual who admitted to participating in a violent crime that may have caused physical harm to a victim; or (iii) for law enforcement authorities to identify or apprehend an individual that appears to have escaped from a correctional institution or from lawful custody.

4. HIPAA does not guarantee individuals the right to access psychotherapy notes. Parents generally do not have a right of access to psychotherapy notes made by a mental health professional related to the child's mental health treatment.

Exhibit Z
Policy and Procedure

POLICY TITLE: Security Rule: Data Integrity and Transmission Security	**POLICY NUMBER:**
ORIGINAL ISSUE DATE: **REVIEW DATES:** **REVISION DATES:** **PAGES:**	**REVIEWED AND APPROVED BY:**

PURPOSE

Children's Dentistry of Amarillo adopts this policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related Security Standards regarding the security and integrity of all electronic protected health information (EPHI). In particular, the purpose of this policy and procedure is to govern data integrity controls to ensure that EPHI is not altered or destroyed in an unauthorized manner or during transmission.

POLICY

Children's Dentistry of Amarillo will establish and maintain appropriate data integrity controls and procedures.

SOURCE

45 C.F.R. § 164.312

PROCEDURE

Data Integrity

1. The Security Officer is responsible for developing and implementing data integrity controls and associated procedures.

2. The Security Officer will develop specific procedures to specify the appropriate use and application of data integrity controls for all information systems, including computers and workstations, which access EPHI.

3. To ensure data is not corrupted, altered or destroyed in an unauthorized manner, members of the workforce will have a level of access appropriate to their

responsibilities and will be limited to the minimum necessary to accomplish his or her workforce tasks.

4. The Security Officer will document all data integrity controls-related activities and procedures.

Transmission Security

1. The Security Officer will identify all methods currently uses to transmit EPHI and implement transmission control procedures to guard against unauthorized access to EPHI that is being transmitted by unauthorized information technology systems. Transmission control procedures can include:

   A. Internet firewalls;

   B. Use of encryption technology; and

   C. Controls on remote access.

2. All electronic transmissions will be made in accordance with this policy and follow data integrity control procedures.