ACADEMY OF DENTAL LEARNING & OSHA TRAINING

# Patient Records: HIPAA & HITECH Best Practices in Dentistry

The Academy of Dental Learning and OSHA Training, LLC, designates this activity for 3 continuing education credits (3 CEs).

Reviewed and Updated by Health Science Editor: Megan Wright, RDH, MS

Publication Date: January 2013

Updated Date: February 2020

Expiration Date: February 2023

ADA C·E·R·P® | Continuing Education Recognition Program

The Academy of Dental Learning and OSHA Training, LLC *is an ADA CERP Recognized Provider. ADA CERP is a service of the American Dental Association to assist dental professionals in identifying quality providers of continuing dental education. ADA CERP does not approve or endorse individual courses or instructors, nor does it imply acceptance of credit hours by boards of dentistry. Concerns or complaints about a CE provider may be directed to the provider or to the Commission for Continuing Education Provider Recognition at ADA.org/CERP.*

Conflict of Interest Disclosure: ADL does not accept promotional or commercial funding in association with its courses. In order to promote quality and scientific integrity, ADL's evidence-based course content is developed independent of commercial interests. Refund Policy: If you are dissatisfied with the course for any reason, prior to taking the test and receiving your certificate, return the printed materials within 15 days of purchase and we will refund your full tuition. Shipping charges are nonrefundable.

California Registered Provider Number: RP5631

# Answer Sheet: Patient Records: HIPAA & HITECH Best Practices in Dentistry

1. _____ 6. _____
2. _____ 7. _____
3. _____ 8. _____
4. _____ 9. _____
5. _____ 10. _____

**Name:** _____ **Profession:** _____

**License State:** _____ **License Number:** _____ **Expiration Date** _____

**Address** _____

**City:** _____ **State:** _____ **Zip Code:** _____

**Telephone:**_____ **Fax:** _____

**E-mail:** _____

**If you have downloaded the course and printed the answer sheet from the Internet please enter payment information below.**

**Card type:** _____ **Card Number:**_____

**Exp. Date:** _____ **Name as it appears on card:** _____

***To enter your answers online you MUST return to our website www.dentallearning.org.**

Return answer sheet:

- Via fax: 518.514.1103
- Via email: CESupport@dentallearning.com
- Postal Mail: ADL, PO Box 14585, Albany, NY 12212

***PLEASE PRINT CLEARLY; ILLEGIBLE ANSWER SHEETS WILL NOT BE PROCESSED.

Notes:

## Course Evaluation

| **Please place an X in the box to rate these statements:** | **Poor** | **Fair** | **Good** | **Very Good** | **Excellent** |
|---|---|---|---|---|---|
| The content fulfills the overall purpose of the course. | | | | | |
| The content fulfills each of the course objectives. | | | | | |
| The course subject matter is accurate. | | | | | |
| The material presented is understandable. | | | | | |
| The teaching/learning method is effective. | | | | | |
| The answers to the test questions are appropriately covered in the course. | | | | | |
| How would you rate this course overall? | | | | | |
| Time to complete the entire course and the test? | **Hours:** _____ | | | **Minutes:** _____ | |
| | **Google** | | | | |
| | **Other Search Engine** | | | | |
| | **Friend/Coworker** | | | | |
| | **Other** | | | | |
| Do you have any suggestions about how we can improve this course? If so please note them on a separate sheet of paper and send it in with your answer sheet. | | | | | |
| If you studied the course online, did all the links work? If not please note the page and link on a separate sheet of paper and send it in with your answer sheet so we can fix it. | | | | | |

## Instructions

1. Review the Objectives: Objectives provide an overview of the entire course.
2. Read the course material.
3. Complete the test:
    a. Return to our website: www.dentallearning.org, click on Take the Exam, enter your answers, register, if you are new customer (existing customers login), pay for the course, click Grade Test. Your test will be graded immediately. If required, complete the course evaluation. Your certificate will display for you to print.
    b. If you would rather, you may return your completed answer sheet and course evaluation to us via the options listed below.

To successfully complete the course you must score 80% or above on the test. If you do not score 80% you may retake the test one more time free of charge. If you fail a second time you must purchase a new course and test.

If you've downloaded this coursebook off the Internet you can:

- Return to our website (www.dentallearning.org) to take the test online (only if you have not purchased the coursebook separately). You will need to provide credit card information at the time you submit your test online for scoring.
- Write your answers on the one-page answer sheet included in this book, complete the credit card payment information, and return the form to the address below, fax, or email address below. Or, you may send a check or money order to the address below with your answer sheet.

    Academy of Dental Learning and OSHA Training, LLC (ADL)
    P.O. Box 14585
    Albany, NY 12212
    Fax: 518-514-1103
    Email: CESupport@dentallearning.org

Answer sheets received without payment will not be processed.

We grade all tests in a timely manner; if you do not receive your certificate within five days, please email (CESupport@dentallearning.org) or call us: 518-209-9540.

There is no time limit for return of your answer sheet. Completion dates are taken from the envelope postmark or the finish date recorded in the computer when you do an online exam. Tests MUST be completed in the licensing cycle you wish to use the credits.

If you are dissatisfied with the course for any reason, prior to taking the test and receiving your certificate, return the printed materials within 15 days of purchase and we will refund your full tuition. Shipping charges are nonrefundable.

If someone else would like to use this material after you are done, he or she may register with us and take advantage of a “sharing discount”. Courses downloaded from the Internet can be shared at the same tuition rate as currently available on our website. Please call us if you need an extra answer sheet or download one from our website. There is no “sharing discount” for online exams.

## Table of Contents

## Objectives

Upon completion of this course, the student will be able to:

- Describe SOAP notes.
- Describe laws relating to patients' rights regarding records access.
- Describe patients' rights to amend their records and learn how to do so correctly.
- Describe who (other than the patient) may access a patient's records and under what circumstances these entities may have access.
- Describe a disclosure log.
- Describe patient notification requirements when a suspected breach of personal health or financial information has occurred.
- Describe state and federal mandates for records retention and disposal.
- Describe best practices for transferring records in a dental practice sale.

## Introduction

Both state and federal law regulate the management of patient records and the information contained therein. Federal laws include the Health Insurance Portability and Accountability Act (HIPAA) and its amendments, the most recent of which is the Health Information Technology for Clinical Health (HITECH) Act of 2009. Other state laws address patient access to health records, security breach notice requirements, and use of health information for marketing purposes. Information and resources for complying with HIPAA and HITECH are available online through The ADA Practical Guide to HIPAA Compliance: Privacy and Security (2020).

## Content and Format of Patient Records

State Dental Practice Acts have specific requirements of treatment entries in patient charts.

Every dentist, dental health profession, or other licensed health professional who performs services on patients in a dental office shall identify him or herself in patient records by signing his or her name, or by writing his or her identification number and initials next to services performed and shall date those treatment entries in the record. If an identification number system is used, a master log of all employees' identification numbers must be maintained in the practice. Many offices choose to use dental license numbers as unique identification numbers.

***Altering patient records with intent to deceive is unprofessional conduct. Correct entries use single-line strikeouts and note the date the correction was made. Do not use opaque correction fluid or tape. It should be clear that there is no attempt to hide information.***

State law also requires that if dental offices solely use electronic recordkeeping systems, they must use an offsite backup storage system, an image mechanism that is able to copy signature documents, and a mechanism to ensure that recorded entries are unalterable. Dentists must develop and implement policies and procedures that include safeguards to protect confidentiality and unauthorized access to electronically stored records, authentication by electronic signature keys, and systems maintenance. Original hard copies of patient records may be destroyed once records have been electronically stored. Computerized record printouts shall be considered as originals.

Liability insurance companies and professional practice standards dictate best practices to follow for determining what information should be kept in patient records. The use of SOAP (subjective, objective, assessment, and plan) notes is highly recommended.

- **Subjective** notes include patients' descriptions of their own health condition and history.
- **Objective** notes include x-rays, examinations, and test findings.
- **Assessment** notes include diagnoses or a list of other possible diagnoses.
- **Plan** notes are recommended treatments or treatment options. Plan notes may also include a summary and outcome of your discussion with a patient.

A widely known professional liability insurance company, The Dentists Insurance Company (TDIC), recommends complete records include:

- A description of the patient's original condition
- Your diagnosis and treatment plan
- Progress notes on the treatment performed and the result of that treatment
- Patient's personal information
- Medical history (all questions answered) and regular updates
- Oral cancer screening and TMJ evaluation
- Diagnostic test findings and exam notes
- Consultant reports, reports to and from specialists, and physicians
- Notes objectively describing complaints or confrontations
- Notes about rescheduled, missed, or canceled appointments
- Exam and treatment notes
- Informed consent conversations and forms
- Models
- All radiographs taken at intervals appropriate to the patient's condition

- Correspondence to/from the patient inclusive of phone calls, e-mails, voice messages, letters, and face-to-face conversations

The outside chart cover should display only the patient's name and/or account number. A color-coded system is recommended if clinical staff think it necessary to have a method to alert them to a patient's health status that will affect dental treatment. For example, a colored sticker on the outside front of the chart can prompt the dentist or hygienist to more closely read patient records.

## Patient Access to Records

A patient record may include any written document in the chart, (even if non-clinical), x-rays, photographs, and models. Access to patient records may not be withheld due to unpaid bills.

**REVISED AS OF 2016:**

On the U.S. Department of Health & Human Services website, Jocelyn Samuels, Former Director, Office for Civil Rights says, "HIPAA's right of access is critical to enabling individuals to take ownership of their health and well-being – but this core right is rendered meaningless when individuals cannot afford to pay the fees. These new FAQs clarify that individuals can be charged only a reasonable, cost-based fee for the labor and supplies associated with making the copy, whether on paper or in electronic form."

**Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524**

**Inspection**

| | |
|---|---|
| Upon written request, a patient or patient's representative has the right to inspect the patient's records. Record inspection should take place during business hours and within five working days of receiving a written request. It is advisable to have an office employee present when the patient or patient's representative inspects records. |  |

Excerpts are copied from: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

## Questions and Answers About HIPAA's Access Right

***A covered entity may not withhold or deny an individual access to her PHI on the grounds that the individual has not paid the bill for health care services the covered entity provided to the individual.***

## Fees That Can Be Charged to Individuals for Copies of their PHI

*May a covered entity charge individuals a fee for providing the individuals with a copy of their PHI?*

Yes, but only within specific limits. The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee to provide the individual (or the individual's personal representative) with a copy of the individual's PHI, or to direct the copy to a designated third party. The fee may include only the cost of certain labor, supplies, and postage:

1. Labor for copying the PHI requested by the individual, whether in paper or electronic form. Labor for copying includes only labor for creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, once the PHI that is responsive to the request has been identified, retrieved or collected, compiled and/or collated, and is ready to be copied. Labor for copying does not include costs associated with reviewing the request for access; or searching for and retrieving the PHI, which includes locating and reviewing the PHI in the medical or other record, and segregating or otherwise preparing the PHI that is responsive to the request for copying.

   While it has always been prohibited to pass on to an individual labor costs related to search and retrieval, our experience in administering and enforcing the HIPAA Privacy Rule has shown there is confusion about what constitutes a prohibited search and retrieval cost and this guidance further clarifies this issue. This clarification is important to ensure that the fees charged reflect only what the Department considers "copying" for purposes of applying 45 CFR 164.524(c)(4)(i) and do not impede individuals' ability to receive a copy of their records.

2. Supplies for creating the paper copy (e.g., paper, toner) or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media. However, a covered entity may not require an individual to purchase portable media; individuals have the right to have their

PHI e-mailed or mailed to them upon request.

3. Labor to prepare an explanation or summary of the PHI, if the individual in advance both chooses to receive an explanation or summary and agrees to the fee that may be charged.

4. Postage, when the individual requests that the copy, or the summary or explanation, be mailed.

Thus, costs associated with updates to or maintenance of systems and data, capital for data storage and maintenance, labor associated with ensuring compliance with HIPAA (and other applicable law) in fulfilling the access request (e.g., verification, ensuring only information about the correct individual is included, etc.) and other costs not included above, even if authorized by State law, are not permitted for purposes of calculating the fees that can be charged to individuals. See 45 CFR 164.524(c)(4).

Further, while the Privacy Rule permits the limited fee described above, covered entities should provide individuals who request access to their information with copies of their PHI free of charge. While covered entities should forgo fees for all individuals, not charging fees for access is particularly vital in cases where the financial situation of an individual requesting access would make it difficult or impossible for the individual to afford the fee. Providing individuals with access to their health information is a necessary component of delivering and paying for health care. We will continue to monitor whether the fees that are being charged to individuals are creating barriers to this access, will take enforcement action where necessary, and will reassess as necessary the provisions in the Privacy Rule that permit these fees to be charged.

*What labor costs may a covered entity include in the fee that may be charged to individuals to provide them with a copy of their PHI?*

A covered entity may include reasonable labor costs associated only with the: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; and (2) labor to prepare an explanation or summary of the PHI, if the individual in advance both chooses to receive an explanation or summary and agrees to the fee that may be charged.

Labor for copying includes only labor for creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, once the PHI that is responsive to the request has been identified, retrieved or collected, compiled

and/or collated, and is ready to be copied. For example, labor for copying may include labor associated with the following, as necessary to copy and deliver the PHI in the form and format and manner requested or agreed to by the individual:

- Photocopying paper PHI.
- Scanning paper PHI into an electronic format.
- Converting electronic information in one format to the format requested by or agreed to by the individual.
- Transferring (e.g., uploading, downloading, attaching, burning) electronic PHI from a covered entity's system to a web-based portal (where the PHI is not already maintained in or accessible through the portal), portable media, e-mail, app, personal health record, or other manner of delivery of the PHI.
- Creating and executing a mailing or e-mail with the responsive PHI.

While we allow labor costs for these limited activities, we note that as technology evolves and processes for converting and transferring files and formats become more automated, we expect labor costs to disappear or at least diminish in many cases.

In contrast, labor for copying does not include labor costs associated with:

- Reviewing the request for access.
- Searching for, retrieving, and otherwise preparing the responsive information for copying. This includes labor to locate the appropriate designated record sets about the individual, to review the records to identify the PHI that is responsive to the request and to ensure the information relates to the correct individual, and to segregate, collect, compile, and otherwise prepare the responsive information for copying.

*May a covered health care provider charge a fee under HIPAA for individuals to access the PHI that is available through the provider's EHR technology that has been certified as being capable of making the PHI accessible?*

No. The HIPAA Privacy Rule at 45 CFR 164.524(c)(4) permits a covered entity to charge a reasonable, cost-based fee that covers only certain limited labor, supply, and postage costs that may apply in providing an individual with a copy of PHI in the form and format requested or agreed to by the individual. Where an individual requests or agrees to access her PHI available through the View, Download, and Transmit functionality of the CEHRT, we believe there are no labor costs and no costs for supplies to enable such access. Thus, a covered health care provider cannot charge an individual a fee when it fulfills an individual's HIPAA access request using the View, Download, and Transmit functionality of the provider's CEHRT.

*May a covered entity that uses a business associate to act on individual requests for access pass on the costs of outsourcing this function to individuals when they request copies of their PHI?*

No. A covered entity may charge individuals a reasonable, cost-based fee that includes only labor for copying the PHI, costs for supplies, labor for creating a summary or explanation of the PHI if the individual requests a summary or explanation, and postage, if the PHI is to be mailed. See 45 CFR 164.524(c)(4). Administrative and other costs associated with outsourcing the function of responding to individual requests for access cannot be the basis for any fees charged to individuals for providing that access.

*Must a covered entity inform individuals in advance of any fees that may be charged when the individuals request a copy of their PHI?*

Yes. When an individual requests access to her PHI and the covered entity intends to charge the individual the limited fee permitted by the HIPAA Privacy Rule for providing the individual with a copy of her PHI, the covered entity must inform the individual in advance of the approximate fee that may be charged for the copy. An individual has a right to receive a copy of her PHI in the form and format and manner requested, if readily producible in that way, or as otherwise agreed to by the individual. Since the fee a covered entity is permitted to charge will vary based on the form and format and manner of access requested or agreed to by the individual, covered entities must, at the time such details are being negotiated or arranged, inform the individual of any associated fees that may impact the form and format and manner in which the individual requests or agrees to receive a copy of her PHI. The failure to provide advance notice is an unreasonable measure that may serve as a barrier to the right of access. Thus, this requirement is necessary for the right of access to operate consistent with the HIPAA Privacy Rule. Further, covered entities should post on their web sites or otherwise make available to individuals an approximate fee schedule for regular types of access requests. In addition, if an individual requests, covered entities should provide the individual with a breakdown of the charges for labor, supplies, and postage, if applicable, that make up the total fee charged. We note that this information would likely be requested in any action taken by OCR in enforcing the individual right of access, so entities will benefit from having this information readily available.

*How can covered entities calculate the limited fee that can be charged to individuals to provide them with a copy of their PHI?*

The HIPAA Privacy Rule permits a covered entity to charge a reasonable, cost-based fee for individuals (or their personal representatives) to receive (or direct to a third party) a copy of the individuals' PHI. In addition to being reasonable, the fee may include only certain labor, supply, and postage costs that may apply in providing the individual with

the copy in the form and format and manner requested or agreed to by the individual. The following methods may be used, as specified below, to calculate this fee.

- Actual costs. A covered entity may calculate actual labor costs to fulfill the request, as long as the labor included is only for copying (and/or creating a summary or explanation if the individual chooses to receive a summary or explanation) and the labor rates used are reasonable for such activity. The covered entity may add to the actual labor costs any applicable supply (e.g., paper, or CD or USB drive) or postage costs. Covered entities that charge individuals actual costs based on each individual access request still must be prepared to inform individuals in advance of the approximate fee that may be charged for providing the individual with a copy of her PHI. An example of an actual labor cost calculation would be to time how long it takes for the workforce member of the covered entity (or business associate) to make and send the copy in the form and format and manner requested or agreed to by the individual and multiply the time by the reasonable hourly rate of the person copying and sending the PHI. What is reasonable for purposes of an hourly rate will vary depending on the level of skill needed to create and transmit the copy in the manner requested or agreed to by the individual (e.g., administrative level labor to make and mail a paper copy versus more technical skill needed to convert and transmit the PHI in a particular electronic format).

- Average costs. In lieu of calculating labor costs individually for each request, a covered entity can develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests, as long as the types of labor costs included are the ones which the Privacy Rule permits to be included in a fee (e.g., labor costs for copying but not for search and retrieval) and are reasonable. Covered entities may add to that amount any applicable supply (e.g., paper, or CD or USB drive) or postage costs.
    - This standard rate can be calculated and charged as a per page fee only in cases where the PHI requested is maintained in paper form and the individual requests a paper copy of the PHI or asks that the paper PHI be scanned into an electronic format. Per page fees are not permitted for paper or electronic copies of PHI maintained electronically. OCR is aware that per page fees in many cases have become a proxy for fees charged for all types of access requests – whether electronic or paper – and that many states with authorized fee structures have not updated their laws to account for efficiencies that exist when generating copies of information maintained electronically. This practice has resulted in fees being charged to individuals for copies of their PHI that do not appropriately reflect the

permitted labor costs associated with generating copies from information maintained in electronic form. Therefore, OCR does not consider per page fees for copies of PHI maintained electronically to be reasonable for purposes of 45 CFR 164.524(c)(4).

- Flat fee for electronic copies of PHI maintained electronically. A covered entity may charge individuals a flat fee for all requests for electronic copies of PHI maintained electronically, provided the fee does not exceed $6.50, inclusive of all labor, supplies, and any applicable postage. **Charging a flat fee not to exceed $6.50 is therefore an option for entities that do not want to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically.**

*Is $6.50 the maximum amount that can be charged to provide individuals with a copy of their PHI?*

No. For any request from an individual, a covered entity (or business associate operating on its behalf) may calculate the allowable fees for providing individuals with copies of their PHI: (1) by calculating actual allowable costs to fulfill each request; or (2) by using a schedule of costs based on average allowable labor costs to fulfill standard requests. Alternatively, in the case of requests for an electronic copy of PHI maintained electronically, covered entities may: (3) charge a flat fee not to exceed $6.50 (inclusive of all labor, supplies, and postage). **Charging a flat fee not to exceed $6.50 per request is therefore an option available to entities that do not want to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically.**

In some cases where an entity chooses generally to use the average cost method, or chooses a flat fee, as described above, for electronic copies of PHI maintained electronically, the entity may receive an unusual or uncommon type of request that it had not considered in setting up its fee structure. In these cases, the entity may wish to calculate actual costs to provide the requested copy, and it may do so as long as the costs are reasonable and only of the type permitted by the Privacy Rule. An entity that chooses to calculate actual costs in these circumstances still must—as in other cases—inform the individual in advance of the approximate fee that may be charged for providing the copy requested.

*Are costs authorized by State fee schedules permitted to be charged to individuals when providing them with a copy of their PHI under the HIPAA Privacy Rule?*

No, except in cases where the State authorized costs are the same types of costs permitted under 45 CFR 164.524(c)(4) of the HIPAA Privacy Rule, and are reasonable.

The bottom line is that the costs authorized by the State must be those that are permitted by the HIPAA Privacy Rule and must be reasonable. The HIPAA Privacy Rule at 45 CFR 164.524(c)(4) permits a covered entity to charge a reasonable, cost-based fee that covers only certain limited labor, supply, and postage costs that may apply in providing an individual with a copy of PHI in the form and format requested or agreed to by the individual. Thus, labor (e.g., for search and retrieval) or other costs not permitted by the Privacy Rule may not be charged to individuals even if authorized by State law. Further, a covered entity's fee for providing an individual with a copy of her PHI must be reasonable in addition to cost-based, and there may be circumstances where a State authorized fee is not reasonable, even if the State authorized fee covers only permitted labor, supply, and postage costs. For example, a State-authorized fee may be higher than the covered entity's cost to provide the copy of PHI. In addition, many States with authorized fee structures have not updated their laws to account for efficiencies that exist when generating copies of information maintained electronically. Therefore, these State authorized fees for copies of PHI maintained electronically may not be reasonable for purposes of 45 CFR 164.524(c)(4).

*A State law requires that a health care provider give individuals one free copy of their medical records but HIPAA permits the provider to charge a fee. Does HIPAA override the State law?*

No, so the health care provider must comply with the State law and provide the one free copy. In contrast to State laws that authorize higher or different fees than are permitted under HIPAA, HIPAA does not override those State laws that provide individuals with greater rights of access to their health information than the HIPAA Privacy Rule does. See 45 CFR 160.202 and 160.203. This includes State laws that: (1) prohibit fees to be charged to provide individuals with copies of their PHI; or (2) allow only lesser fees than what the Privacy Rule would allow to be charged for copies.

*When do the HIPAA Privacy Rule limitations on fees that can be charged for individuals to access copies of their PHI apply to disclosures of the individual's PHI to a third party?*

The fee limits apply when an individual directs a covered entity to send the PHI to the third party. Under the HIPAA Privacy Rule, a covered entity is prohibited from charging an individual who has requested a copy of her PHI more than a reasonable, cost-based fee for the copy that covers only certain labor, supply, and postage costs that may apply in fulfilling the request. See 45 CFR 164.524(c)(4). This limitation applies regardless of whether the individual has requested that the copy of PHI be sent to herself, or has directed that the covered entity send the copy directly to a third party designated by the individual (and it doesn't matter who the third party is). To direct a copy to a third party, the individual's access request must be in writing, signed by the individual, and clearly identify the designated person or entity and where to send the PHI. See 45 CFR

164.524(c)(3)(ii). Thus, written access requests by individuals to have a copy of their PHI sent to a third party that include these minimal elements are subject to the same fee limitations in the Privacy Rule that apply to requests by individuals to have a copy of their PHI sent to themselves. This is true regardless of whether the access request was submitted to the covered entity by the individual directly or forwarded to the covered entity by a third party on behalf and at the direction of the individual (such as by an app being used by the individual). Further, these same limitations apply when the individual's personal representative, rather than the individual herself, has made the request to send a copy of the individual's PHI to a third party.

In contrast, third parties often will directly request PHI from a covered entity and submit a written HIPAA authorization from the individual (or rely on another permission in the Privacy Rule) for that disclosure. Where the third party is initiating a request for PHI on its own behalf, with the individual's HIPAA authorization (or pursuant to another permissible disclosure provision in the Privacy Rule), the access fee limitations do not apply. However, as described above, where the third party is forwarding - on behalf and at the direction of the individual - the individual's access request for a covered entity to direct a copy of the individual's PHI to the third party, the fee limitations apply.

We note that a covered entity (or a business associate) may not circumvent the access fee limitations by treating individual requests for access like other HIPAA disclosures – such as by having an individual fill out a HIPAA authorization when the individual requests access to her PHI (including to direct a copy of the PHI to a third party). As explained elsewhere in the guidance, a HIPAA authorization is not required for individuals to request access to their PHI, including to direct a copy to a third party – and because a HIPAA authorization requests more information than is necessary or that may not be relevant for individuals to exercise their access rights, requiring execution of a HIPAA authorization may create impermissible obstacles to the exercise of this right. Where it is unclear to a covered entity, based on the form of a request sent by a third party, whether the request is an access request initiated by the individual or merely a HIPAA authorization by the individual to disclose PHI to the third party, the entity may clarify with the individual whether the request was a direction from the individual or a request from the third party. OCR is open to engaging with the community on ways that technology could easily convey this information.

Finally, we note that disclosures to a third party made outside of the right of access under other provisions of the Privacy Rule still may be subject to the prohibition against sales of PHI (i.e., the prohibition against receiving remuneration for a disclosure of PHI at 45 CFR 164.502(a)(5)(ii)). Where the prohibition applies, a covered entity may charge only a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI or a fee otherwise expressly permitted by other law or must have received a HIPAA authorization from the individual that states that the disclosure will involve remuneration

to the covered entity.

*May a health care provider withhold a copy of an individual's PHI from the individual who requested it because the covered entity used the individual's payment of the allowable fee for the copy to instead pay an outstanding bill for health care services provided to the individual?*

No. Just as a covered entity may not withhold or deny an individual access to his PHI on the grounds that the individual has not paid the bill for health care services the covered entity provided to the individual, a covered entity may not withhold or deny access on the grounds that the covered entity used the individual's payment of the fee for a copy of his PHI to offset or pay the individual's outstanding bill for health care services.

*Can an individual be charged a fee if the individual requests only to inspect her PHI at the covered entity (i.e., does not request that the covered entity produce a copy of the PHI)?*

No. The fees that can be charged to individuals exercising their right of access to their PHI apply only in cases where the individual is to receive a copy of the PHI, versus merely being provided the opportunity to view and inspect the PHI. The HIPAA Privacy Rule provides individuals with the right to inspect their PHI held in a designated record set, either in addition to obtaining copies or in lieu thereof, and requires covered entities to arrange with the individual for a convenient time and place to inspect the PHI. See 45 CFR 164.524(c)(1) and (c)(2). Consequently, covered entities should have in place reasonable procedures to enable individuals to inspect their PHI, and requests for inspection should trigger minimal additional effort by the entity, particularly where the PHI requested is of the type easily accessed onsite by the entity itself in the ordinary course of business. For example, covered entities could use the capabilities of Certified EHR Technology (CEHRT) to enable individuals to inspect their PHI, if the individuals agree to the use of this functionality.

Further, a covered entity may not charge an individual who, while inspecting her PHI, takes notes, uses a smart phone or other device to take pictures of the PHI, or uses other personal resources to capture the information. If the individual is making the copies of PHI using her own resources, the covered entity may not charge a fee for those copies, as the copying is being done by the individual and not the entity. A covered entity may establish reasonable policies and safeguards regarding an individual's use of her own camera or other device for copying PHI to assure that equipment or technology used by the individual is not disruptive to the entity's operations and is used in a way that enables the individual to copy or otherwise memorialize only the records to which she is entitled. Further, a covered entity is not

required to allow the individual to connect a personal device to the covered entity's systems.

**X-rays**

*Do individuals have a right under HIPAA to get copies of their x-rays or other diagnostic images, and if so, in what format?*

Yes. An individual has a right to receive PHI about the individual maintained by a covered entity in a designated record set, such as a medical record. See 45 CFR 164.524(a)(1). This includes x-rays or other images in the record. As with other PHI in a designated record set, the individual has a right to access the information in the form and format she requests, as long as the covered entity can readily produce it in that form and format. See 45 CFR 164.524(c). The large file size of some x-rays or other images may impact the mechanism for access (e.g., the format agreed upon by the individual and the covered entity must accommodate the file size).

## Summary of Records

State law allows healthcare providers discretion to provide a summary of a patient's records to a patient requesting a copy of the record. However, a dental practice that is a HIPAA-covered entity may prepare a summary of a patient's record only if the patient has approved the action in advance. A records summary shall be made available to the patient within 10 working days from date of request. More time may be allowed to prepare a summary if the record is large, but the summary must be provided within 30 days of request.

Under the HIPAA Privacy Rule, a covered entity must act on an individual's request for access no later than 30 calendar days after receipt of the request. If the covered entity is not able to act within this timeframe, the entity may have up to an additional 30 calendar days, as long as it provides the individual – within that initial 30-day period – with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request. See 45 CFR 164.524(b)(2).

***Allowable Charges (Summary of Records)***

Dentists may charge no more than reasonable fees based on actual time and costs incurred for summary preparation.

**Public Benefit Program Appeal**

If a patient requires a copy of a portion of his or her record to support an appeal regarding eligibility for a public benefit program the copy shall be provided by the dental

office at no charge.

***Allowable Charges***

The patient is entitled to no more than one copy free of charge but may not be limited in the number of requests for copies.

## Transmission of Records

*Do individuals have the right under HIPAA to have copies of their PHI transferred or transmitted to them in the manner they request, even if the requested mode of transfer or transmission is unsecure?*

Yes, as long as the PHI is "readily producible" in the manner requested, based on the capabilities of the covered entity and transmission or transfer in such a manner would not present an unacceptable level of security risk to the PHI on the covered entity's systems, such as risks that may be presented by connecting an outside system, application, or device directly to a covered entity's systems (as opposed to security risks to PHI once it has left the systems). For example, individuals generally have a right to receive copies of their PHI by mail or e-mail, if they request. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail and transmitting PHI in such a manner does not present unacceptable security risks to the systems of covered entities, even though there may be security risks to the PHI once it has left the systems. Thus, a covered entity may not require that an individual travel to the covered entity's physical location to pick up a copy of her PHI if the individual requests the copy be mailed or e-mailed. In the limited case where a covered entity is unable to e-mail the PHI as requested, such as in the case where diagnostic images are requested and e-mail cannot accommodate the file size of the images, the covered entity should offer the individual alternative means of receiving the PHI, such as on portable media that can be mailed to the individual.

Further, while covered entities are required by the Privacy and Security Rules to implement reasonable safeguards to protect PHI while in transit, individuals have a right to receive a copy of their PHI by unencrypted e-mail if the individual requests access in this manner. In such cases, the covered entity must provide a brief warning to the individual that there is some level of risk that the individual's PHI could be read or otherwise accessed by a third party while in transit, and confirm that the individual still wants to receive her PHI by unencrypted e-mail. If the individual says yes, the covered entity must comply with the request. We note that providers using the 2015 edition of Certified EHR Technology will have the capability to send unencrypted e-mail transmissions directly from that technology.

Whether an individual has a right to receive a copy of her PHI through other unsecure

modes of transmission or transfer (assuming the individual requests the mode and accepts the risk) depends on the extent to which the mode of transmission or transfer is within the capabilities of the covered entity and the mode would not present an unacceptable level of risk to the security of the PHI on the covered entity's systems (as explained above), based on the covered entity's Security Rule risk analysis. For example, a covered entity's risk analysis may provide that connecting an outside (foreign) device, such as a USB drive, directly to the entity's systems presents an unacceptable level of risk to the PHI on the systems. In this case, the covered entity is not required to agree to an individual's request to transfer the PHI in this manner, but the entity must offer some other means of providing electronic access to the PHI.

Note that while an individual can receive copies of her PHI by unsecure methods if that is her preference, as described in more detail above, a covered entity is not permitted to require an individual to accept unsecure methods of transmission in order to receive copies of her health information.

*Is a covered entity responsible if it complies with an individual's access request to receive PHI in an unsecure manner (e.g., unencrypted e-mail) and the information is intercepted while in transit?*

No. While covered entities are responsible for adopting reasonable safeguards in implementing the individual's request (e.g., correctly entering the e-mail address), covered entities are not responsible for a disclosure of PHI while in transmission to the individual based on the individual's access request to receive the PHI in an unsecure manner (assuming the individual was warned of and accepted the risks associated with the unsecure transmission). This includes breach notification obligations and liability for disclosures that occur in transit. Further, covered entities are not responsible for safeguarding the information once delivered to the individual. Covered entities are responsible for breach notification for unsecured transmissions and may be liable for impermissible disclosures of PHI that occur in all contexts except when fulfilling an individual's right of access under 45 CFR 164.524 to receive his or her PHI or direct the PHI to a third party in an unsecure manner.

*Do individuals have a right under HIPAA to have their PHI downloaded on portable media that they provide?*

Whether PHI is "readily producible" for purposes of providing access will depend on the extent to which the requested method of copying, transfer, or transmission is within the capabilities of the covered entity and would not present an unacceptable level of risk to the security of the PHI on the covered entity's systems, based on the covered entity's Security Rule risk analysis.

With respect to portable media supplied by an individual, covered entities are required

by the Security Rule to perform a risk analysis related to the potential use of external portable media and are not required to accept the external media if they determine there is an unacceptable level of risk to the PHI on their systems. However, covered entities are not then permitted to require individuals to purchase a portable media device from the covered entity if the individual does not wish to do so. The individual may in such cases opt to receive an alternative form of the electronic copy of the PHI, such as through email.

**Right to Have PHI Sent Directly to a Designated Third Party**

*Can an individual, through the HIPAA right of access, have his or her health care provider or health plan send the individual's PHI to a third party?*

Yes. If requested by an individual, a covered entity must transmit an individual's PHI directly to another person or entity designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person or entity and where to send the PHI. See 45 CFR 164.524(c)(3)(ii). A covered entity may accept an electronic copy of a signed request (e.g., PDF or scanned image), an electronically executed request (e.g., via a secure web portal) that includes an electronic signature, or a faxed or mailed copy of a signed request.

The same requirements for providing the PHI to the individual, such as the timeliness requirements, fee limitations, prohibition on imposing unreasonable measures, and form and format requirements, apply when an individual directs that the PHI be sent to another person or entity. For example, just as when the individual requests a copy for herself, a covered entity cannot require that an individual make a separate in person trip to the covered entity's physical location for the purpose of making the request to transmit the individual's PHI to a person or entity designated by the individual. In addition, the individual can designate the form and format of the PHI and how the PHI is to be sent to the third party, and the covered entity must provide access in the requested form and format and manner if the PHI is "readily producible" in such a way. Whether PHI is "readily producible" depends on the capabilities of the covered entity and whether transmission or transfer of the PHI in the requested manner would present an unacceptable level of security risk to the PHI on the covered entity's systems (based on the covered entity's Security Rule risk analysis).

*Are there any limits or exceptions to the individual's right to have the individual's PHI sent directly to a third party?*

The right of an individual to have PHI sent directly to a third party is an extension of the individual's right of access; consequently, all of the provisions that apply when an individual obtains access to her PHI apply when she directs a covered entity to send the PHI to a third party. As a result:

- This right applies to PHI in a designated record set;
- Covered entities must take action within 30 days of the request;
- Covered entities must provide the PHI in the form and format and manner of access requested by the individual if it is “readily producible” in that manner; and
- The individual may be charged only a reasonable, cost-based fee that complies with 45 CFR 164.524(c)(4).

Further, the same limited grounds for denial of access that apply when the individual is receiving the PHI directly apply in cases where the individual requests that the PHI be provided to a designated third party. See 45 CFR 164.524(a)(2) and (a)(3). Thus, for example, a covered entity may deny an individual’s request to send PHI to a designated third party when the request is for psychotherapy notes or PHI for which a licensed health care professional has determined, exercising professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. The provisions of the Privacy Rule providing for review of certain denials of access apply in this circumstance as well. See 45 CFR 164.524(a)(3) and (a)(4). However, a covered entity may not deny an individual’s access request to send PHI to a third party for other purposes. Thus, disagreement with the individual about the worthiness of the third party as a recipient of PHI, or even concerns about what the third party might do with the PHI (except for the express reasons listed in the Privacy Rule, such as in cases where life or physical safety is threatened), are not acceptable reasons to deny an individual’s request.

## Patient Requests to Amend Records

Both HIPAA and state law provide patients the right to request amendments to their records. However, laws differ in how a healthcare provider can respond to such a request. Ideally, a discussion with the patient regarding an amendment should be done prior to initiation of the amendment process. Once a written request for amendment is submitted, the dentist must respond.

Under HIPAA, patients submit requests to the covered entity to amend their records. The healthcare provider may require a written request and reason for the amendment be submitted. The provider should respond within 60 days of receiving a request but may have another 30 days if an extension is requested in advance from the patient.

When a patient’s request is granted, notify the patient of your decision in writing. Make amendments to records without destroying previously entered information. Add notations regarding dates of amendments and reasons. Provide amended information to entities identified by patients and others who the provider knows have legitimate need for this information.

A provider can deny a patient's request **only** under the following circumstances:

- The information proposed to be amended is accurate and complete.
- The information may not be accessed by the patient.
- The information was not created by the provider unless the provider knows the original information provider is no longer available.
- The information is not part of the patient record.

When the patient's request is denied, notify the patient in writing of your decision. Include your reason and an explanation for your denial in the notification. The patient must also be informed of other rights, including the right to file a complaint with the U.S. Department of Health and Human Services. For additional information, sample policies and forms, refer to The ADA Practical Guide to HIPAA Compliance: Privacy and Security Kit (2010).

**Denial of Access**

*Grounds for Denial*

Under certain limited circumstances, a covered entity may deny an individual's request for access to all or a portion of the PHI requested. In some of these circumstances, an individual has a right to have the denial reviewed by a licensed health care professional designated by the covered entity who did not participate in the original decision to deny.

*Unreviewable* grounds for denial (45 CFR 164.524(a)(2)):

- The request is for psychotherapy notes, or information compiled in reasonable anticipation of, or for use in, a legal proceeding.
- An inmate requests a copy of her PHI held by a covered entity that is a correctional institution, or health care provider acting under the direction of the institution, and providing the copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of correctional officers, employees, or other person at the institution or responsible for the transporting of the inmate. However, in these cases, an inmate retains the right to inspect her PHI.
- The requested PHI is in a designated record set that is part of a research study that includes treatment (e.g., clinical trial) and is still in progress, provided the individual agreed to the temporary suspension of access when consenting to participate in the research. The individual's right of access is reinstated upon completion of the research.
- The requested PHI is in Privacy Act protected records (i.e., certain records under the control of a federal agency, which may be maintained by a federal

agency or a contractor to a federal agency), if the denial of access is consistent with the requirements of the Act.

- The requested PHI was obtained by someone other than a health care provider (e.g., a family member of the individual) under a promise of confidentiality, and providing access to the information would be reasonably likely to reveal the source of the information.

*Reviewable* grounds for denial (45 CFR 164.524(a)(3)). A licensed health care professional has determined in the exercise of professional judgment that:

- The access requested is reasonably likely to endanger the life or physical safety of the individual or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g., concerns that the individual will not be able to understand the information or may be upset by it).
- The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
- The provision of access to a personal representative of the individual that requests such access is reasonably likely to cause substantial harm to the individual or another person.

Note that a covered entity may <u>not require</u> an individual to provide a reason for requesting access, and the individual's rationale for requesting access, if voluntarily offered or known by the covered entity or business associate, is <u>not</u> a permitted reason to deny access. In addition, a covered entity may not deny access because a business associate of the covered entity, rather than the covered entity itself, maintains the PHI requested by the individual (e.g., the PHI is maintained by the covered entity's electronic health record vendor or is maintained by a records storage company offsite).

*Carrying Out the Denial*

If the covered entity denies access, in whole or in part, to PHI requested by the individual, the covered entity must provide a denial in writing to the individual no later than within 30 calendar days of the request (or no later than within 60 calendar days if the covered entity notified the individual of an extension). See 45 CFR 164.524(b)(2). The denial must be in plain language and describe the basis for denial; if applicable, the individual's right to have the decision reviewed and how to request such a review; and how the individual may submit a complaint to the covered entity or the HHS Office for Civil Rights. See 45 CFR 164.524(d).

If the covered entity (or one of its business associates) does not maintain the PHI requested, but knows where the information is maintained, the covered entity must inform the individual where to direct the request for access. See 45 CFR 164.524(d)(3).

The covered entity must, to the extent possible and within the above timeframes, provide the individual with access to any other PHI requested, after excluding the PHI to which the entity has a ground to deny access. See 45 CFR 164.524(d)(1). Complexity in segregating the PHI does not excuse the obligation to provide access to the PHI to which the ground for denial does not apply.

*Review of Denial*

If the denial was based on a reviewable ground for denial and the individual requests review, the covered entity must promptly refer the request to the designated reviewing official. The reviewing official must determine, within a reasonable period of time, whether to reaffirm or reverse the denial. The covered entity must then promptly provide written notice to the individual of the determination of the reviewing official, as well as take other action as necessary to carry out the determination. See 45 CFR 164.524(d)(4).

***A covered entity may not withhold or deny an individual access to her PHI on the grounds that the individual has not paid the bill for health care services the covered entity provided to the individual.***

Under both federal and state law, information may not be removed from a patient's record under any circumstance. Corrections should be done using single-line strikeouts, and the date the correction was made should be noted. Do not use opaque correction fluid or tape. It should be clear there is no attempt to hide information.

**~~Use single line strikeout.~~**

## Upon a Dentist's Death or Incapacitation

A dentist who has been contracted by the estate or trust of a dentist who has died or become incapacitated, shall obtain a form signed by the deceased or incapacitated dentist's patient, or the patient's legal guardian, that releases the patient's dental records to the contracting dentist or dentists prior to use of those records.

## Access to Patient Records by other Entities

Records can be released to anyone a patient chooses as long as the dental office receives written authorization signed by the patient or his or her representative and if the dentist determines that releasing records will not cause the patient harm. Authorization forms should specify who is to receive records and any limitations regarding release of records or information.

Restricted and confidential health information with regard to pregnancy, HIV test results, sexually transmitted diseases, mental health, and alcohol or drug abuse may not be

provided to a requestor without specific patient consent. If an entity other than a patient is not requesting information or records, the dentist must, based on HIPAA law, determine if the requestor may have the information.

### Other Healthcare Professionals

HIPAA allow dental practices to provide patient information without patient authorization to other healthcare professionals as long as the purpose of the information is to provide treatment.

Although HIPAA Privacy Rules allow the use and transfer of patient information to relevant parties who need information for healthcare operations and during sales of dental practices, state law does not include similar provisions. In the transfer, sale, merger, or consolidation of a dental practice, it is prudent for the seller to obtain written patient authorization prior to allowing a buyer or partner to view charts. The absent provision in state law also means that a new practice owner should stay on the safe side of state privacy laws, and obtain written patient authorization before using patient records.

If a patient sets an appointment with the new dentist, he or she implies authorization allowing the new dentist to view his or her dental records. Patient authorizations must be separate from acknowledgements of the office's Notice of Privacy Practices. Authorization forms may be mailed to patients together with the selling dentist's notification of transferring practice ownership.

In the transfer, sale, merger, or consolidation of a dental practice, the new owner may agree to custody of patient records (the alternative is that the former owner retains records). As custodian of records, the owner is legally responsible for ensuring records are secure, and if records are to be destroyed, owners must ensure that records are unreadable.

### Employers

Employers, in general, do not have the right to access patient records except in workers' compensation cases or when necessary to carry out responsibilities for workplace medical surveillance under federal or state mandates. Employers who self-insure may have limited access to patient information necessary to determine payment. Employer-sponsored dental benefit plan representatives also have limited access to patient information necessary to determine payment and to conduct quality assessment audits.

**Payers**

If an individual other than the patient is financially responsible for a patient's bill, disclosure of patient information is allowed as long as disclosures are limited to the minimum information necessary to obtain payment. In making such disclosures, healthcare providers also must honor reasonable requests for confidential communications and any agreed-to restrictions on the use or disclosure of patients' protected health information.

The dental office's Notice of Privacy Practices can state if a patient designates another person as responsible for payment, the office will disclose a minimum amount of personal health information necessary to obtain payment from that person. If a patient objects to that disclosure, the office should inform the patient that he or she must choose between allowing information disclosure (in order to obtain payment) or self-payment.

If a patient pays full cost out-of-pocket for an item or service and requests personal health information regarding the item or service not be disclosed to a health plan for purposes of payment or healthcare operations, the dental office must honor the patient's request.

**Parents – Divorced or Separated**

A parent generally has a right to access his or her minor child's health record irrespective of custody or financial responsibility. A dental practice may refuse to give access to a parent if it determines providing access may harm the patient. A parent does not have a right to access emancipated minors' health records. An emancipated minor is an individual under 18 yrs old who is either (a) married or divorced, (b) on active duty with the U.S. armed forces; or (c) received a declaration of emancipation from the court.

**Former Associate Dentists**

A former Associate Dentist may not copy or otherwise use patient health information from a previously affiliated practice without first obtaining written authorization from patients.

**Representative of Deceased Patient**

A legally designated representative or beneficiary of a deceased patient may inspect or obtain copies of records. A representative or beneficiary may also grant third-parties access to records. Dental offices should request verification of requestor's status as a deceased patient's representative or beneficiary. A proposed HIPAA rule would allow dentists discretion regarding release of information to family members or individuals

involved in a patient's care or patient's payment for care.

**Subpoenas**

Subpoenas are valid if:

- Personally served on you or someone authorized by you to receive a subpoena
- Issued by the clerk of the court or attorney handling the lawsuit
- Addressed to you or someone qualified to certify the requested records
- It contains a date specified for production of records that is at least 20 days after issuance, 15 days after it was served on you, and 20 days after the subpoena was received
- It specifies each item or category of items to be produced
- It contains documentation demonstrating that the patient has either consented to a release of records or has been informed of the records request
- The 20 days is specified, because time is allowed for the court to hear motions to suppress

If a subpoena is valid and you are not a party to the lawsuit, produce records as requested, sign the affidavit and submit a statement for costs incurred for responding to the subpoena.

**Marketing Activity**

HIPAA limits the use of protected health information for marketing activities on behalf of covered entities or third parties.

**Mandated Reporting**

Licensed dental professionals' disclosure obligations regarding domestic abuse, criminal activity, and other legal violations involving patients is not hindered in any way by HIPAA.

**Patient's Right to Know about Disclosures**

A patient has the right to receive an accounting of disclosures of personal health information by healthcare providers who are HIPAA covered entities. The disclosure must be provided within 60 days of the request, although the patient may grant (upon request and given reason for delay), a 30-day extension. No fee can be charged for the first disclosure-accounting log in a 12-month period. If it is stated in the dental office's Notice of Privacy Practices, a reasonable fee can be charged for subsequent disclosure-accounting logs requested in the same 12-month period. The subsequent disclosure-accounting log can be provided after the fee is paid. The contents of a

disclosure accounting log should contain the following elements:

- Disclosure dates
- Name and contact information of entities receiving information
- Description of information disclosed
- Purpose of disclosure or copy of the request
- If there are multiple disclosures to the same entity of the same type of information, the frequency of disclosures during the accounting period and the date of the last disclosure

A patient's right to an accounting may be suspended for one of two reasons–belief that the patient may be endangered (e.g., domestic violence situations) or upon request by law enforcement.

The HITECH Act expanded disclosure accounting rules to include HIPAA business associates. In addition, covered entities who maintain electronic health records (EHRs) are now required to provide an accounting of more types of disclosures than covered entities who do not use EHRs. However, the Department of Health and Human Services has not yet adopted regulations implementing this law, so specifics regarding accounting logs and the implementation date are unknown at this time.

Disclosure-accounting logs, names and titles of dental professionals responsible for receiving and processing requests for disclosure accountings must be retained for six years. For more information and sample forms on disclosures accounting, refer to The ADA Practical Guide to HIPAA Compliance: Privacy and Security Kit (2010). Your office policies and procedures should describe how you manage patient requests for disclosure-accountings.

**Data Breach Notification Requirements**

A healthcare provider is required to notify patients when an actual or suspected breach of personal health or financial information has occurred.

**Records Retention and Disposal**

State law does not define the period of time dentists must maintain patient records after patients discontinue treatment. Un-emancipated minors' records shall be kept at least one year after a minor has reached 18 years and in any case not less than seven years. Contact your professional liability carrier for recommendations. Ideally, all dental records, active and inactive, should be maintained indefinitely. Records must be kept for seven years after a dental practice closes.

Maintain all parts of records, including radiographs and models. If onsite, inactive-patient records storage is not an option, store records offsite in a secure location, or

store records electronically. A patient who has not returned for treatment within 24-36 months is considered inactive. Separate inactive, adult-patient files from inactive, minor-patient files.

Patient records should be shredded or disposed of in a manner that makes personal information unreadable or indecipherable. **Failure to destroy records in a manner that preserves patient confidentiality violates state law**. Persons injured because a dentist abandons patient records may bring action in court against the licensee, partnership, or corporation.

If hiring a records disposal company, it is recommended you choose one that specializes in destroying records by burning or shredding. Radiographs should be separated from paper files and, due to film silver content, disposed of through a silver recycler, hazardous waste vendor, or household hazardous waste program that accepts small business, hazardous waste. A log should be kept indicating dates and descriptions of destroyed records. This log will assist you in the event destroyed records are requested.

Transferring Records in a Sale

If you are selling or transferring your practice, it is important to remember to:

1. Transfer responsibility and liability for proper storage and disposal of records to the new practice owner.
2. Ensure your continued access to those records for an indefinite time period in case of litigation.

**Recent HIPAA Changes & How to Revise Your Business Associate Agreements**

Jeff Drummond explains, in his online publication in *D Healthcare Daily*, "When HIPAA was originally enacted and the first set of regulations published, the statutory language specified that only certain 'Covered Entities' would be required to abide by the law: health care providers, health insurance plans, and specialty health data entities known as health care clearinghouses. That left many entities with regular access to medical information, such as billing companies, accountants, lawyers, pharmacy benefit management companies, and other healthcare entities and vendors, outside the scope of the law. The original HIPAA regulations offered a fix for this conundrum: 'Covered Entities' are required to enter into agreements with the 'Business Associates' to whom they provide medical information; these 'Business Associate Agreements' or 'BAAs' impose by contract the same HIPAA obligations that are imposed on the Covered Entities by statute and regulation.

When the HITECH Act provisions were published as part of the Stimulus Bill, HIPAA was amended so that Business Associates are now directly liable for most HIPAA requirements. So, no more BAAs, right? Wrong; because the HITECH Act only imposed some obligations on Business Associates, and because a Business Associate's obligations need to be closely tailored to the covered entity for which it works, BAAs are still necessary. Additionally, the HITECH Act (and the recently published 'Omnibus Rule' regulations implementing it) add some specific provisions that should be included in a Covered Entity's BAAs.

The US Department of Health and Human Services provided a form of BAA back when the original regulations was published, and has developed a new set of 'Sample BAA Provisions' which are available here: [http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html] . Every BAA must impose ten primary criteria on Business Associates:

1. What uses and disclosures are permitted;
2. No other uses or disclosures unless specifically allowed;
3. Implement appropriate safeguards;
4. Report breaches and problems;
5. Assist Covered Entity with granting individuals' access, amendment, and accounting of disclosures;
6. Comply with other requirements applicable to Covered Entity;
7. Make available books and records to HHS;
8. At termination, return or destroy all information;
9. Ensure that subcontractors meet the same standards; and
10. Authorize termination if the Business Associate breaches the BAA.

Of course, if you are a covered entity, you probably already have a BAA that you've used regularly since the early days of HIPAA, and you'd like to keep as much of your current contract as possible. If so, all you need to do is amend your existing BAA to include all of the new requirements of HITECH and the Omnibus Rule. Specifically, you need to amend your BAA to add the following provisions:

1. Add a definition of HITECH and the Omnibus Rule, and consider whether to include them in the definition of HIPAA.
2. Where the BAA describes the Business Associate as an entity receiving data from the Covered Entity or producing it for the Covered Entity, include the words 'creates, receives, maintains or transmits.' That is the new language defining the roles that a third party vendor can play to become a Business Associate, and it is useful to include the same language.
3. Specifically note that the Business Associate must notify you of any 'breach' as defined in HIPAA. This can be included in the 'reporting of disclosures'

section or some similar location. Remember to include a relatively short reporting period (3-5 days, usually), so that you will be able to meet your own timing requirements if the breach must be reported. A Covered Entity has up to 60 days to report a breach, but that is an outside limit; the obligation is to report 'without unreasonable delay' and if your Business Associate delays in reporting to you, you may not be able to meet your own timing constraints. You may be treated as knowing of the breach at the same time the Business Associate discovers it, not when they report it to you.

4. Add to the 'accounting of disclosures' section a statement specifying that, if the Business Associate maintains records in electronic form, it will account for ALL disclosures for at least a 3-year period. This is different from the original accounting requirement, which excludes many disclosures but lasts for 6 years.
5. Specifically note that the Business Associate has obligations under the HITECH Act, and require the Business Associate to acknowledge and agree to abide by those requirements.
6. Add a provision noting that the Business Associate will abide by requirements not to disclose data to insurers and other health plans if the patient pays for the service in full and requests confidentiality. The Covered Entity will likely have to notify the Business Associate that a patient has requested such secrecy.
7. The BAA should already give the Covered Entity right to terminate if the Business Associate violates the BAA. However, you should add a provision allowing the Business Associate to terminate the BAA if the Covered Entity fails to meet its HIPAA obligations. This is not mentioned in the Omnibus Rule, but was specifically noted in the HITECH Act.
8. The Omnibus Rule added some language to the BAA regulations that was not otherwise mentioned in the HITECH Act. If the Business Associate carries out one of the Covered Entity's obligations under the Privacy Rule, the BAA must require that the Business Associate agree to abide by that Privacy Rule provision. While this is covered conceptually in almost every BAA already, it can't hurt to include specific language to this effect.

The HITECH Act and the Omnibus Rule also require Covered Entities to review their Notices of Privacy Practices and in most cases make some revisions."

**HIPAA Breach Notification Rule**

Excerpt taken from https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

**Definition of Breach**

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information 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.

Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.

There are three exceptions to the definition of “breach.” The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person 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. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception applies if the covered entity or business associate

has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

**Unsecured Protected Health Information and Guidance**

Covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

This guidance was first issued in April 2009 with a request for public comment. The guidance was reissued after consideration of public comment received and specifies encryption and destruction as the technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Additionally, the guidance also applies to unsecured personal health record identifiable health information under the FTC regulations. Covered entities and business associates, as well as entities regulated by the FTC regulations, that secure information as specified by the guidance are relieved from providing notifications following the breach of such information.

**Breach Notification Requirements**

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

**Individual Notice**

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

**Media Notice**

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

**Notice to the Secretary**

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

### Notification by a Business Associate

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

### Administrative Requirements and Burden of Proof

Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."

Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

### Recent Breach in the News

Excerpt taken from https://www.hhs.gov/about/news/2017/01/18/hipaa-settlement-demonstrates-importance-implementing-safeguards-ephi.html

> **FOR IMMEDIATE RELEASE**
> **January 9, 2017**
> **Contact: HHS Press Office**
> **202-690-6343**
> **media@hhs.gov**
>
> **First HIPAA enforcement action for lack of timely breach notification settles for $475,000:**
>
> The U.S. Department of Health and Human Services, Office for Civil Rights

(OCR), has announced the first Health Insurance Portability and Accountability Act (HIPAA) settlement based on the untimely reporting of a breach of unsecured protected health information (PHI). Presence Health has agreed to settle potential violations of the HIPAA Breach Notification Rule by paying $475,000 and implementing a corrective action plan. Presence Health is one of the largest health care networks serving Illinois and consists of approximately 150 locations, including 11 hospitals and 27 long-term care and senior living facilities. Presence also has multiple physicians' offices and health care centers in its system and offers home care, hospice care, and behavioral health services. With this settlement amount, OCR balanced the need to emphasize the importance of timely breach reporting with the desire not to disincentive breach reporting altogether.

On January 31, 2014, OCR received a breach notification report from Presence indicating that on October 22, 2013, Presence discovered that paper-based operating room schedules, which contained the PHI of 836 individuals, were missing from the Presence Surgery Center at the Presence St. Joseph Medical Center in Joliet, Illinois. The information consisted of the affected individuals' names, dates of birth, medical record numbers, dates of procedures, types of procedures, surgeon names, and types of anesthesia. OCR's investigation revealed that Presence Health failed to notify, without unreasonable delay and within 60 days of discovering the breach, each of the 836 individuals affected by the breach, prominent media outlets (as required for breaches affecting 500 or more individuals), and OCR.

"Covered entities need to have a clear policy and procedures in place to respond to the Breach Notification Rule's timeliness requirements" said OCR Director Jocelyn Samuels. "Individuals need prompt notice of a breach of their unsecured PHI so they can take action that could help mitigate any potential harm caused by the breach."

The Resolution Agreement and Corrective Action Plan may be found on the OCR website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/presence

OCR's guidance on breach notification may be found at http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

## Conclusion

Federal and state law, primarily through the HIPAA and HITECH Acts, and CMIA, mandate how entities covered by these laws must protect, handle, store, and dispose of patient records. These laws describe patient record formatting and content, patients'

rights regarding records access and amendment, who (other than the patient) may access records and under what circumstances each entity may have access, disclosure logs and patient notification requirements when a suspected breach may have occurred, and best practices for transferring records in a dental practice sale. To avoid litigation, healthcare providers must protect patient information, privacy, and records security by following federal and state law. If you have any further questions, information and resources for complying with HIPAA and HITECH are available online through The ADA Practical Guide to HIPAA Compliance: Privacy and Security.

## References


ADA Practical Guide to HIPAA Compliance: Privacy and Security (2020).

Business and Professions Code §§ 1680(s), 1683, 1684.1

Drummond, Jeff. “HIPAA Changes: How to Revise Your Business Associate Agreements.” *D Healthcare Daily, Government/Law*. January 27,2017

Health & Safety Code §§123100-123149.5, 130200-130205

Health Information Technology for Clinical Health (HITECH) Act - 2009

Health Insurance  Portability and Accountability Act

U.S. Department of Health & Human Services. “HIPAA FOR PROFESSIONALS.” Website: www.hhs.gov/hipaa/for-professionals/index.html Date Accessed: February 2020.

## Course Test: Patient Records: HIPPA and HITECH Best Practices in Dentistry

1. SOAP notes include all of the following, **except**:

    a. The patient's description of his or her health condition and history
    b. X-rays, examination notes and test findings
    c. Records disclosure dates
    d. Recommended treatment options

2. Upon written request, patients have the right to receive copies of their records within:

    a. 30 days
    b. 10 days
    c. Immediately
    d. 5 days

3. When a patient's request for records amendment is granted, you must destroy all previous notes which may be contradictory to amendments.

    a. True
    b. False

4. This entity is entitled to full access to patient records:

    a. Employees
    b. Former associate dentists
    c. Parents
    d. Payors

5. Subpoenas are valid if all of the following are true, **except**:

    a. Issued by the court
    b. Personally served on you
    c. Addressed to you
    d. Contains a date specified for producing records that is at least 15 days after issuance

6. Disclosure logs must be retained for:

    a. 7 years
    b. 6 years
    c. 10 years
    d. 5 years

7. Healthcare providers are required to notify patients when an actual or suspected breach of personal health or financial information has occurred.

    a. True
    b. False

8. Un-emancipated minor's records shall be kept at least one year after the minor has reached the age of 18 years, and in any case, not less than seven years.

    a. True
    b. False

9. Best practices for transferring records in a dental practice sale require dental practitioners to transfer responsibility and liability for proper storage and disposal of records to a new practice owner, but do not require previous owners' continued access to those records.

    a. True
    b. False

10. A summary of records may only be prepared:

    a. By a HIPAA covered entity
    b. If a patient approves the action in advance
    c. Within 15 working days from date of request
    d. By a former associate dentist