



# HIPAA complexities and compliance issues

Second edition

A peer-reviewed article written by Richard H. Nagelberg, DDS

PUBLICATION DATE: JANUARY 2020

EXPIRATION DATE: DECEMBER 2022

# HIPAA complexities and compliance issues

## ABSTRACT

The Health Insurance Portability and Accountability Act (HIPAA) is well known to all health-care providers and everyone who has visited any health-care facility. The need to protect the personal and medical information of patients is the primary reason for the enactment of HIPAA in 1996. HIPAA is very complex, making compliance difficult. Additionally, patient comanagement and communication among a variety of facilities, including labs, specialists, diagnostic and imaging centers, among many others, has further complicated compliance across the spectrum of patient care. Companies that facilitate secure communication and assistance with HIPAA compliance provide protection for covered entities and the patient as well.

## EDUCATIONAL OBJECTIVES

At the conclusion of this educational activity, participants will be able to:

1. Describe the basic HIPAA regulations
2. Discuss HIPAA updates
3. Define “individually identifiable health information” and “covered entities”
4. Discuss secure communication among facilities participating in patient care



Dental Academy of Continuing Education™

Go online to take this course.  
**DentalAcademyofCE.com**

QUICK ACCESS CODE 15423

This continuing education (CE) activity was developed by the PennWell dental group, an operating unit of Endeavor Business Media, with no commercial support.

This course was written for dentists, dental hygienists, and dental assistants, from novice to skilled.

**Educational methods:** This course is a self-instructional journal and web activity.

**Provider disclosure:** Endeavor Business Media neither has a leadership position nor a commercial interest in any products or services discussed or shared in this educational activity, nor with the commercial supporter. No manufacturer or third party had any input in the development of the course content.

**Requirements for successful completion:** To obtain three CE credits for this educational activity, you must pay the required fee, review the material, complete the course evaluation, and obtain a score of at least 70%.

**CE planner disclosure:** Laura Winfield, Endeavor Business Media dental group CE coordinator, neither has a leadership nor commercial interest with the products or services discussed in this educational activity. Ms. Winfield can be reached at lwinfield@endeavor2b.com

**Educational disclaimer:** Completing a single continuing education course does not provide enough information to result in the participant being an expert in the field related to the course topic. It is a combination of many educational courses and clinical experience that allows the participant to develop skills and expertise.

**Image authenticity statement:** The images in this educational activity have not been altered.

**Scientific integrity statement:** Information shared in this CE course is developed from clinical research and represents the most current information available from evidence-based dentistry.

**Known benefits and limitations of the data:** The information presented in this educational activity is derived from the data and information contained in reference section. The research data is extensive and provides a direct benefit to the patient and improvements in oral health.

**Registration:** The cost of this CE course is \$59 for three CE credits.

**Cancellation and refund policy:** Any participant who is not 100% satisfied with this course can request a full refund by contacting Endeavor Business Media in writing.



Endeavor Business Media  
Nationally Approved PACE Program  
Provider for FAGD/MAGD credit.  
Approval does not imply acceptance  
by any regulatory authority or AGD  
endorsement. 11/1/2019 to 10/31/2022.  
Provider ID# 320452

Endeavor designates this activity for 3 continuing educational credits.

Dental Board of California: Provider 4527, course registration number CA code: 03-4527-15423

*"This course meets the Dental Board of California's requirements for 3 units of continuing education."*

Endeavor Business Media is designated as an approved PACE program provider by the Academy of General Dentistry (AGD). The formal continuing dental education programs of this program provider are accepted by the AGD for fellowship, mastership, and membership maintenance credit. Approval does not imply acceptance by a state or provincial board of dentistry or AGD endorsement. The current term of approval extends from (11/1/2019) to (10/31/2022) Provider ID# 320452.



Endeavor/PennWell Corporation is designated as an approved Provider by the American Academy of Dental Hygiene Inc. # AADHPNW (January 1, 2019–December 31, 2020). Approval does not imply acceptance by a state or provincial Board of Dentistry. Licensee should maintain this document in the event of an audit.

**ADA CERP®** | Continuing Education  
Recognition Program

Endeavor Business Media 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 ADA CERP at [ada.org/goto/cerp](http://ada.org/goto/cerp).



## INTRODUCTION

The primary purpose of the Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, is to protect all individually identifiable health information held or transmitted by a covered entity in any form or medium, including electronic, paper, and oral forms. HIPAA provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.<sup>1</sup>

This course will discuss HIPAA regulations and available strategies to facilitate patient care among different providers, while adhering to the requirements to protect patient information. It will also discuss why email is not adequate to meet these needs. The primary goal is to provide optimal care for patients without violating the privacy of their health-care information.

## WHAT IS THE HIPAA PRIVACY RULE?

In its most basic form, the HIPAA Privacy Rule indicates who is covered, what information is protected, and how protected health information can be used and disclosed. According to the U.S. Department of Health and Human Services, “The Standards for Privacy of Individually Identifiable Health Information (‘Privacy Rule’) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (‘HHS’) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (‘HIPAA’). The Privacy Rule standards address the use and disclosure of individuals’ health information—called ‘protected health information’ by organizations subject to the Privacy Rule—called ‘covered entities,’ as well as standards for individuals’ privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights (‘OCR’) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties. A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well

being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.”<sup>1</sup>

## COVERED ENTITIES

Covered entities are health plans including health insurance companies and employer-sponsored health plans, health-care clearinghouses, and health-care providers who engage in defined electronic transactions that commonly relate to insurance reimbursement. The types of electronic transactions that require compliance with the Privacy Rule include claims, benefit eligibility confirmation, and referral authorizations. Examples of covered entities include private physicians, dentists, laboratories, social workers, hospitals, ambulances/EMTs, pharmacists, administrative staff members who handle protected information, and any other person or organization that furnishes, bills, or is paid for health care.

According to HHS, “The HIPAA Privacy Rule protects most ‘individually identifiable health information’ held or transmitted by a covered entity or its business associate, in any form or medium. The Privacy Rule calls this information ‘protected health information’ (PHI). Protected health information is information, including demographic information, which relates to:

- the individual’s past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.”<sup>1</sup>

One of the primary purposes of the Privacy Rule is to define the circumstances in which protected health information can be used or disclosed by covered entities. There

are two requirements that must be adhered to regarding use or disclosure of protected health information. The first is that such information may not be used or disclosed except as the Privacy Rule permits or as the individual authorizes in writing. Secondly, disclosure of protected health information is required if an individual requests access to his or her records or if HHS requests the information.

Another aspect of the use of protected health information is the principle of “minimum necessary.”<sup>2</sup> The covered entity must make reasonable effort to disclose the minimum information necessary to comply with the request, disclosure, or use of the information.

## COMPLEXITY OF REQUIREMENTS AND REGULATIONS

There are many regulatory bodies and a considerable amount of legislation that is concerned with patient privacy in the US. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) protects the privacy of patient information.<sup>3</sup> Other aspects of HIPAA include the Health Information Technology for Economic and Clinical Health Act (HITECH), public interest and benefit activities, health oversight activities, incidental use and disclosure, judicial and administrative proceedings, law enforcement purposes, decedents, worker’s compensation, hybrid entities, and minors, among many others.<sup>1</sup> There is considerable overlap among these varied considerations and requirements, further complicating the ability of covered entities to be compliant.

There are instances in which a covered entity can provide treatment or care solely to generate protected health information for disclosure to a third party. An example of this is a physician conducting a physical examination for a life insurance carrier. The results of the physical examination are transmitted to the life insurance company, with the patient’s permission. Another example is treatment provided during the clinical trial phase of research. With an individual’s permission, the protected health information can be used or disclosed for the research. In these two examples, authorization is provided by the individual conditionally—i.e., for the sole purpose of generating the protected

health-care information—and the authorization only provides for use or disclosure to the life insurance carrier or for research purposes.

The original intent of HIPAA was to simplify and streamline health-care delivery. Title I of HIPAA protects the health-care insurance of individuals when they lose or change jobs. Title II is known as the Administrative Simplification (AS) provisions. This section of the law requires the establishment of national standards for electronic health-care transactions and national identifiers for providers, employers, and health insurance plans.

## ELECTRONIC EXCHANGE OF INFORMATION

The law also sets standards for electronic exchange of patient information and includes protecting the privacy of that information. This includes information relating directly or indirectly to the person's past, present, or future physical or mental health, the provision of care to the person, and the person's health-care bills, demographic information, and payments. A covered entity does not have to keep health information confidential when the information does not reveal the identity of an individual and when the individual authorizes the release of information in a written, HIPAA-compliant authorization.<sup>4</sup>

Small covered entities, such as private dental and medical practices, must comply to the same extent as large, multistate health plans with hundreds or thousands of employees and dedicated compliance and human resources (HR) departments. When patient information must be transmitted among providers (or other covered entities), such as family practice dentists and physicians and specialists, it must be done in a secure manner. Common sources of audits are the patients themselves. Compliance includes both consent and security.

## TRADITIONAL EMAIL IS NOT COMPLIANT

A patient cannot consent to unsecure email transmission of their protected information to another provider. To be compliant with the requirement for securing the patient's information, protocols and controls must

be in place, which ensure that access to the information cannot be accomplished easily. These controls may take the form of user ID; encryption; identity authentication; data backup, storage, and disposal; among others. Traditional email communication will pass through dozens of servers and does not have the controls necessary to fulfill the requirements for compliance. Furthermore, there must be an auditable record of the individuals who were able to read, write, and delete patient information. Compliance also requires procedures to be in place to address the final disposal of the protected patient information. The discovery of most deviations from HIPAA compliance comes from a patient or individual whose information has been handled improperly.

None of the traditional technologies, including Hotmail/Outlook, Gmail, Dropbox, and SkyDrive/OneDrive, are compliant with HIPAA requirements at the time of this writing. Similarly, confidentiality notices on traditional email do not provide compliance. Text and voice messages containing PHI are also vulnerable and do not comply with secure communication requirements.

## SECURE SOLUTIONS

Even simple, everyday functions in a dental office require HIPAA compliance. Every time there is a laboratory prescription for a prosthesis, including handwritten or electronically transmitted prescriptions, HIPAA compliance is required if PHI is included. It must also have an auditable record indicating any parties who were able to read, write, and delete patient information. Disposal of the PHI contained in an electronic communication must also be compliant and auditable.

## HIPAA VIOLATIONS

Patients who suspect their protected health information was misused have the mechanism to make a complaint and trigger an investigation. Most information breaches are due to lost or stolen unencrypted data. Archiving PHI on tape backup systems exposes the information to loss or theft. Cloud-based, HIPAA-compliant backup systems provide secure patient information storage solutions. Legal action has occurred many times for improper data

handling. Some cases involve the disclosure of PHI on social media networks. Other legal actions involve unencrypted backup tapes being stolen from an automobile and instances in which the patient information is mistakenly sent to the wrong recipient who then posts it online. The penalties for HIPAA violations are determined by a schedule of four tiers of increasing severity. Tier 1 penalties are violations in which the covered entity was unaware that the violation occurred. Tier 4 penalties are willful neglect of HIPAA rules. The fines for Tier 1 penalties are \$100–\$25,000 per violation. Tier 4 penalties are subject to fines of \$50,000 per violation.<sup>4</sup>

In 2010, New York–Presbyterian Hospital (NYP) agreed to pay \$3.3 million for a HIPAA violation. NYP disclosed the PHI of 6,800 patients to a number of internet search engines. In a related case, Columbia University agreed to pay \$1.5 million for failure to conduct a thorough risk analysis of all IT equipment and data systems utilizing PHI.

## CONCLUSION

The utilization of the services that ensure HIPAA compliance is increasing as digital technology replaces paper-based health-care records. The conversion to electronic health records creates challenges to handling protected health information in a secure, compliant manner. Failure to comply can result in substantial financial penalties, loss of confidence, and damage to the reputation of the provider. Inadvertent or accidental mishandling of PHI is not defensible and is potentially subject to penalties if a violation occurs. With the availability of services to ensure proper handling of patient information, combined with the complexity of the HIPAA regulations, utilization of these services should be considered by all covered entities.

## REFERENCES

1. Office for Civil Rights. Summary of the HIPAA Privacy Rule. U.S. Department of Health & Human Services website. <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>. Updated July 26, 2013.
2. Redhead CS. HIPAA Privacy, Security, Enforcement, and Breach Notification Standards. Congressional Research Service. <https://fas.org/>



## ONLINE COMPLETION

Take this test online for immediate credit. Go to [dentalacademyofce.com](http://dentalacademyofce.com) and log in. If you do not have an account, sign up using enrollment key **DACE2019**. Then, find this course by searching for the title or the quick access code. Next, select the course by clicking the "ENROLL" option. Continue by pressing "Start." After you have read the course, you may take the exam. Search for the course again and place the exam in your cart. Check out, take the exam, and receive your credit!

## QUESTIONS

1. **The acronym HIPAA stands for:**
  - A. Health Insurance Privacy and Accountability Act
  - B. Health Information Portability and Accountability Act
  - C. Health Insurance Portability and Accountability Act
  - D. Health Information Privacy and Accountability Act
2. **Since implementation of HIPAA:**
  - A. No changes have been made
  - B. There have been some minor updates
  - C. Major updates have occurred annually
  - D. There have been some major updates
3. **Which of the following are covered entities?**
  - A. Pharmacists
  - B. Ambulances
  - C. Social workers
  - D. All of the above
4. **Which of the following activities does not need to comply with the Privacy Rule?**
  - A. Insurance claims
  - B. Written communication with the patient
  - C. Benefit eligibility confirmation
  - D. Referral authorization
5. **Individually identifiable health information includes:**
  - A. The patient's future medical condition
  - B. The patient's past payments for health-care services
  - C. The provision of care for the patient
  - D. All of the above
6. **PHI is an abbreviation for:**
  - A. Protected health information
  - B. Private health information
  - C. Portability of health insurance
  - D. None of the above
7. **Which of the following is true regarding the Privacy Rule?**
  - A. Establishes standards for protection of patient information
  - B. Addresses the use and disclosure of patient information
  - C. Balances the need to protect patient information and permitted use of that information
  - D. All of the above
8. **Enforcement of the Privacy Rule is carried out by the:**
  - A. Office for Civil Regulations
  - B. Office for Patient Rights
  - C. Office for Civil Rights
  - D. Office for HIPAA Compliance
9. **Which of the following are requirements regarding the disclosure of patient information?**
  - A. Patient's verbal authorization
  - B. Use of provider's email for information transmission
  - C. Usage of patient information as the Privacy Rule permits
  - D. All of the above
10. **Title II of HIPAA:**
  - A. Protects the health insurance of individuals when they lose or change jobs
  - B. Is known as the Administrative Simplification (AS) provisions
  - C. Defines covered entities
  - D. All of the above
11. **Which of the following statements is true regarding transmission of health information in which the patient has provided written permission?**
  - A. A covered entity has to keep health information confidential when the information does not reveal the identity of an individual
  - B. A covered entity does not have to keep health information confidential when the information does not reveal the identity of an individual
  - C. A covered entity does not have to keep health information confidential when the information reveals the identity of an individual
  - D. None of the above
12. **Small covered entities such as private dental practices:**
  - A. Do not have to comply as fully as larger covered entities
  - B. Do not have to comply with HIPAA regulations
  - C. Must comply to the same extent as large, multistate health plans
  - D. None of the above
13. **Transmission of PHI among covered entities must be done:**
  - A. In a secure manner
  - B. With the provider's regular email
  - C. With the patient's regular email
  - D. All of the above
14. **In general, HIPAA protects:**
  - A. Companies from unauthorized use of PHI
  - B. Individuals from authorized disclosure of PHI
  - C. Dental labs from authorized use of PHI
  - D. Individuals from unauthorized use of PHI
15. **Protocols that protect patient information during transmission of PHI include:**
  - A. Encryption
  - B. Data backup
  - C. Identity authentication
  - D. All of the above

## ONLINE COMPLETION

Take this test online for immediate credit. Go to [dentalacademyofce.com](http://dentalacademyofce.com) and log in. If you do not have an account, sign up using enrollment key **DACE2019**. Then, find this course by searching for the title or the quick access code. Next, select the course by clicking the "ENROLL" option. Continue by pressing "Start." After you have read the course, you may take the exam. Search for the course again and place the exam in your cart. Check out, take the exam, and receive your credit!

## QUESTIONS

**16. To be compliant with HIPAA regulations:**

- A. Transmitted data does not need to be encrypted
- B. The recipient of the transmission is responsible for final data disposal
- C. There must be an auditable record of the individuals who were able to read, write, and delete patient information
- D. The patient does not need to consent to any form of data transmission

**17. Traditional email does not comply with HIPAA regulations:**

- A. Since the email will pass through dozens of servers
- B. Due to the nonsecure, nonencrypted manner in which data is transmitted
- C. Since there is no secure mechanism for final disposal of the transmitted information
- D. All of the above

**18. The discovery of most deviations from full compliance with HIPAA regulations originates with:**

- A. The Office for Civil Rights
- B. The patient
- C. The U.S. Department of Health and Human Services
- D. The covered entity

**19. The majority of information breaches are the result of:**

- A. Lost data
- B. Stolen data
- C. Unencrypted data
- D. All of the above

**20. Which of the following comply with HIPAA regulations?**

- A. Confidentiality notices on email
- B. Having patients sign a form permitting the usage of traditional email
- C. Text messages
- D. None of the above

**21. Which of the following statements is correct?**

- A. The utilization of the services that ensure HIPAA compliance is increasing
- B. The utilization of the services that ensure HIPAA compliance is decreasing
- C. Conversion to electronic health records simplifies HIPAA compliance
- D. None of the above

**22. The primary purpose of HIPAA is to:**

- A. Protect the health information of groups of people
- B. Protect the health information of individuals
- C. Protect PHI being held or transmitted in any manner
- D. Both B and C

**23. In its most basic form, the HIPAA Privacy Rule indicates:**

- A. Who is covered
- B. The type of information that is protected
- C. Both A and B
- D. Neither A or B

**24. The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to:**

- A. Only define covered entities
- B. Implement HIPAA requirements
- C. Enforce compliance with HIPAA regulations
- D. Ensure no additional regulations are added to HIPAA

**25. The Privacy Rule is designed to be:**

- A. Inflexible to respond to the diverse health-care marketplace
- B. Flexible to respond to the uniformity of the health-care marketplace
- C. Flexible to respond to the diverse health-care marketplace
- D. None of the above

**26. Individually identifiable health information includes:**

- A. Social Security number
- B. Birthdate
- C. Name and address
- D. All of the above

**27. Disclosure of protected health information is required when:**

- A. An individual requests access to his/her records
- B. HHS requests the information
- C. Both A and B
- D. Neither A nor B

**28. The principle of "minimum necessary" addresses the need to:**

- A. Provide as much information as possible to a covered entity
- B. Provide the minimum information necessary to another covered entity
- C. Make minimal effort to provide the minimum necessary information
- D. Provide the minimum necessary information to the patient

**29. Examples of when a covered entity can provide treatment or care solely to generate protected health information include:**

- A. Physical examination for life insurance without the patient's permission
- B. Treatment during clinical trial phase of research
- C. Physical exam for life insurance with the patient's permission
- D. Both B and C

**30. Everyday functions in a dental office that require HIPAA compliance include:**

- A. Laboratory prescriptions
- B. Written pharmacy prescriptions
- C. Insurance billing for services rendered
- D. All of the above

# HIPAA complexities and compliance issues

Name: \_\_\_\_\_ Title: \_\_\_\_\_ Specialty: \_\_\_\_\_

Address: \_\_\_\_\_ Email: \_\_\_\_\_ AGD member ID (if applies): \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ ZIP: \_\_\_\_\_ Country: \_\_\_\_\_

Telephone: Primary ( ) \_\_\_\_\_ Office ( ) \_\_\_\_\_ License renewal date: \_\_\_\_\_

**Requirements for obtaining CE credits by mail/fax:** 1) Read entire course. 2) Complete info above. 3) Complete test by marking one answer per question. 4) Complete course evaluation. 5) Complete credit card info or write check payable to Endeavor Business Media. 6) Mail/fax this page to DACE. A score of 70% is required for CE credit. **For questions, call (800) 633-1681. Course may also be completed at dentalacademyofce.com.**

## EDUCATIONAL OBJECTIVES

- Describe the basic HIPAA regulations
- Discuss HIPAA updates
- Define "individually identifiable health information" and "covered entities"
- Discuss secure communication among facilities participating in patient care

## COURSE EVALUATION

1. Were the individual course objectives met?

Objective #1: Yes No Objective #2: Yes No

Objective #3: Yes No Objective #4: Yes No

Please evaluate this course by responding to the following statements, using a scale of Excellent = 5 to Poor = 0.

2. To what extent were the course objectives accomplished overall? 5 4 3 2 1 0

3. Please rate your personal mastery of the course objectives. 5 4 3 2 1 0

4. How would you rate the objectives and educational methods? 5 4 3 2 1 0

5. How do you rate the author's grasp of the topic? 5 4 3 2 1 0

6. Please rate the instructor's effectiveness. 5 4 3 2 1 0

7. Was the overall administration of the course effective? 5 4 3 2 1 0

8. Please rate the usefulness and clinical applicability of this course. 5 4 3 2 1 0

9. Please rate the usefulness of the supplemental weblography. 5 4 3 2 1 0

10. Do you feel that the references were adequate? Yes No

11. Would you participate in a similar program on a different topic? Yes No

12. If any of the continuing education questions were unclear or ambiguous, please list them.

13. Was there any subject matter you found confusing? Please describe.

14. How long did it take you to complete this course?

15. What additional continuing dental education topics would you like to see?

Mail/fax completed answer sheet to:

**Endeavor Business Media**

Attn: Dental division

7666 E. 61st St. Suite 230, Tulsa, OK 74133

Fax: (918) 831-9804

Payment of \$59 is enclosed.

**Make check payable to Endeavor Business Media**

If paying by credit card, please complete the following:  MC  Visa  AmEx  Discover

Acct. number: \_\_\_\_\_

Exp. date: \_\_\_\_\_ CVC #: \_\_\_\_\_

Billing address: \_\_\_\_\_

**Charges on your statement  
will show up as PennWell / Endeavor.**

- |                     |                     |
|---------------------|---------------------|
| 1. (A) (B) (C) (D)  | 16. (A) (B) (C) (D) |
| 2. (A) (B) (C) (D)  | 17. (A) (B) (C) (D) |
| 3. (A) (B) (C) (D)  | 18. (A) (B) (C) (D) |
| 4. (A) (B) (C) (D)  | 19. (A) (B) (C) (D) |
| 5. (A) (B) (C) (D)  | 20. (A) (B) (C) (D) |
| 6. (A) (B) (C) (D)  | 21. (A) (B) (C) (D) |
| 7. (A) (B) (C) (D)  | 22. (A) (B) (C) (D) |
| 8. (A) (B) (C) (D)  | 23. (A) (B) (C) (D) |
| 9. (A) (B) (C) (D)  | 24. (A) (B) (C) (D) |
| 10. (A) (B) (C) (D) | 25. (A) (B) (C) (D) |
| 11. (A) (B) (C) (D) | 26. (A) (B) (C) (D) |
| 12. (A) (B) (C) (D) | 27. (A) (B) (C) (D) |
| 13. (A) (B) (C) (D) | 28. (A) (B) (C) (D) |
| 14. (A) (B) (C) (D) | 29. (A) (B) (C) (D) |
| 15. (A) (B) (C) (D) | 30. (A) (B) (C) (D) |

AGD code: 566

## PLEASE PHOTOCOPY ANSWER SHEET FOR ADDITIONAL PARTICIPANTS.

### INSTRUCTIONS

All questions have only one answer. Grading of this examination is done manually. Participants will receive confirmation of passing by receipt of a verification form. Verification of Participation forms will be mailed within two weeks after taking an examination.

### COURSE EVALUATION AND FEEDBACK

We encourage participant feedback. Complete the survey above and e-mail feedback to Aileen Gunter (agunter@endeavor2b.com) and Laura Winfield (lwinfield@endeavor2b.com).

### COURSE CREDITS AND COST

All participants scoring at least 70% on the examination will receive a verification form for three CE credits. The formal CE program of this sponsor is accepted by the AGD for fellowship and mastership credit. Please contact Endeavor for current term of acceptance. Participants are urged to contact their state dental boards for continuing education requirements. PennWell is a California CE provider. The California provider number is 4527. The cost for courses ranges from \$20 to \$110.

### PROVIDER INFORMATION

Endeavor 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 neither approves nor endorses individual courses or instructors, nor does it imply acceptance of credit hours by boards of dentistry. Concerns about a CE provider may be directed to the provider or to ADA CERP at [ada.org/goto:cerp/](http://ada.org/goto:cerp/).

Endeavor is designated as an approved PACE program provider by the Academy of General Dentistry. The formal continuing dental education programs of this program provider are accepted by the AGD for fellowship, mastership, and membership maintenance credit. Approval does not imply acceptance by a state or provincial board of dentistry or AGD endorsement. The current term of approval extends from 11/1/2019 to 10/31/2022. Provider ID# 320452.

### RECORD KEEPING

Endeavor maintains records of your successful completion of any exam for a minimum of six years. Please contact our offices for a copy of your CE credits report. This report, which will list all credits earned to date, will be generated and mailed to you within five business days of receipt.

### EDUCATIONAL DISCLAIMER

Completing a single CE course should not provide enough information to give participants the feeling that they are experts in the field related to the course topic. It is a combination of many educational courses and clinical experience that allows the participant to develop skills and expertise.

### CANCELLATION AND REFUND POLICY

Any participant who is not 100% satisfied with this course can request a full refund by contacting Endeavor in writing.

### IMAGE AUTHENTICITY

The images provided and included in this course have not been altered.

© 2019 by the Academy of Dental Therapeutics and Stomatology, a division of Endeavor Business Media