Training Session Handouts

Dental HIPAA: Head Off Front Desk Nightmares

Presented by:
Rhonda Granja, B.S., CMC, CMOM, CMA, CPC

HEALTHCARE TRAINING LEADER®
Expert Medical Practice Solutions

[DISCLAIMER]

This webinar is an independent product of Healthcare Training Leader. It is not endorsed by nor has it any official connection with any other organization, insurance carrier, vendor, or company. Reasonable attempts have been made to provide accuracy in the content. However, of necessity, examples cited and advice given in a national periodical such as this must be general in nature and may not apply to any particular case. The publisher, editors, board members, contributors, nor consultants warrant or guarantee that the information contained herein on coding or compliance will be applicable or appropriate in any particular situation.

Healthcare Training Leader®, 2277 Trade Center Way,
Suite 101, Naples, FL 34109, Phone: 800-767-1181 •
Fax: 800-767-9706 • E-mail: info@trainingleader.com •
Website: www.hctrainingleader.com

Head off Front Desk Dental HIPAA Nightmares

By Rhonda Granja, B.S., CMA, CMC, CMIS, CMOM, CMC, CPC

1

- Dental Practices have been grumbling over HIPAA compliance for over 10 years! Ask any dentist, office manager, receptionist, dental assistant, dental hygienist, dentist spouse, IT professional, or consultant about HIPAA and you will likely receive a negative response that relates to the challenges of HIPAA compliance.

2

- A recent security breach involving a copy machine resulted in a $1.2M fine. Incidents like this scare the average dental practice into questioning whether their compliance program is intact.
- You can be compliant with a little help..

3

HIPAA

- Health Insurance Portability and Accountability Act
- Enacted to:
  - Improve the efficiency and effectiveness of the health care system through the establishment of national standards and requirements for electronic health care transactions
  - To protect the privacy and security of individually identifiable health information
- These are known as HIPAA's Administrative Simplification provisions.

4

HIPAA

- Health Insurance Portability and Accountability Act
- The intent of HIPAA was threefold, to:
  - Provide insurance portability for patients
  - Promote simplification or consistent standards
  - Prevent fraud and abuse of the healthcare system

5

HIPAA

- The law includes provisions
  - Designed to encourage electronic transactions such as claims submission
  - Safeguards and protects the security and confidentiality of patient health information
- Patients also have many new rights and protections against the misuse or disclosure of personal health information

6

HIPAA

- Under these regulations you:
  - Need to evaluate current practice policies and procedures in the protection and submission of all patient health data
  - Accomplish a gap risk analysis of the patient privacy protocols within the practice including the security of patient information and medical records.

7

HIPAA

- PHI: Protected Health Information
  - Anything in the medical record
- IIHI: Individually Identifiable Health Information
  - 19 identifiable items that can identify the patient
- Is the Date of Birth (DOB) PHI or IIHI?

8

HIPAA

- Authorization:
  - For the use of information not in the treatment, payment or healthcare operations (TPO) a valid patient authorization must be obtained.
  - You cannot require a signed authorization in order to provoke treatment.
  - Patient or responsible party may revoke authorization at any time

9

HIPAA

- Common Privacy Violations:
  - Overheard conversations – ie. Receptionist is having a conversation with a patient in your office while scheduling them with an oral surgeon
  - Someone leaves their desk with the computer screen visible
  - PHI/IIHI left on desks or discarded in the trash where janitorial staff or others can view it

10

HIPAA

- Common Privacy Violations
  - Patient sign in sheets that requests reason for the visit with the doctor
  - Phone messages left with spouse, co-workers, or answering machines without consent
  - Dental professional discussing other patients in the office as they flow from room to room

11

Check - In

- Avoid:
  - "Is your insurance still the same?"
  - "Has anything changed?"
- Use:
  - "What is the name of your insurance?"
  - "I need to verify that we have your most current information. What is the ID number printed on your insurance card?"

12

Check - In

- Practice adequately responding to patients:
  - *"It's the same as last time."*
  - "Mrs. Jones, for verification purposes and to protect your identity, we are required to double check the name of your insurance and ID number."

13

Check - In

- Know what forms you are asking the patients to complete.
  - *"What's this for?"*
  - Avoid: "It's the HIPAA form."
  - *"What's that?"*
  - Avoid: "It's the Privacy Form."

14

Check - In

- *"I already signed that."*
- Avoid: *"You need to sign it again."*
- Use: *"According to HIPAA regulations, we are required to provide you an updated Notice of Privacy Practices. Allow me to point out some of the changes…. "*

15

Check - In

- Know your state & federal regulations
- Compliance is not an option!!

- Are you providing your patients the Notice of Privacy Practices Policy and making a good faith effort to obtain a written acknowledgment of the receipt of the Notice of Privacy Practices Policy?

16

Check - In

- An established patient signs in for her appointment and tells the front desk she does not want to bill her insurance and pay out of pocket for the visit.
- A) “Ok. Today’s charges will total…..”
- B) “We have a contractual agreement with your insurance to bill for services rendered.”
- **Refer to “Request to Opt Out” Form.

17

Check - In

- You are in VIOLATION of the HIPAA requirements!!!

18

Check - In

- When providing forms to sign:
- Avoid:
  - *"Please sign here, here, and here."*
- Use:
  - *"Please take a moment to review and sign the financial policy."*

19

Business Associates

- Business associates can be held directly accountable by federal or state authorities for any failure to comply with HIPAA statutory or applicable regulations.
- Make sure that your BAA are updated reflecting the new Omnibus provisions as of 9-23-2014.
- 30-70% of privacy and security breaches involve a vendor. Be sure to verify that the agreement does not disclaim responsibility.

20

Examples of Business Associates

- Billing Services
- Collection agencies
- Computer hardware & software vendors
- Independent contractors
- Consultants
- What about janitorial service providers?

21

What is IIHI?

- Individually Identifiable Health Information
- There are 19 identifiers. A few to mention are:
  - Name
  - Telephone numbers
  - Fax Numbers
  - Social Security Number
  - E-mail Addresses
  - Medical Record numbers
  - Vehicle identifiers
  - Full face photographic images
  - Account numbers

22

Omnibus Rule

- HIPAA received a face lift at the end of 2013. Lots of changes as well as enforcement items were noted..
- Example: Are patient names on dental lab labels a HIPAA violation?
- What about wall to fame bulletin boards or Christmas photo cards?

23

Patient Rights

- Patients will have the right to review PHI/IIHI about themselves and request corrections to errors.
- A covered entity providing direct treatment will be required to:
  - Provide a "notice of privacy practice" to each patient.
  - Outline how health information will be used

24

Patient Rights

- Attempt to obtain written acknowledgement of the receipt of privacy notice.
- Explain patient's right to review information and request corrections.
  - Should correction be denied patient has right to request a statement of disagreement be included as part of the permanent record.
  - Covered entity will have right to file rebuttal to statement should they so choose.
- Explain patient right to limit or restrict disclosure.
- Explain patient right to accounting of disclosures.

25

Identity Theft Alert: RED FLAGS

- The term "Red Flag" has been adopted by the FTC to mean a pattern, practice, or specific activity that indicates the possible existence of IDENTITY THEFT.

26

Red Flags

- Clinical Setting
  - Patient's medical condition doesn't match the medical record.
  - Records are inconsistant with the physical state of the patient or his/her medical history.
  - Records show substantial discrepancies in age, race, sex, or other physical descriptions.

27

Red Flags

- Non-Clinical Setting
  - Inconsistent information or employment records, medical records, or registration information.
  - Documents that appear to be forged or altered (including driver's license, etc)
  - Missing laptops, security codes, equipment with patient or employee information, etc.

28

Spotlight on Social Networking

- In an age where social networking websites, such as Facebook and Twitter are a popular way to communicate, it is important to remember that the internet is a public domain.
- You have an obligation to safeguard PHI regardless of the setting.
- Do not post identifying information about patients or their images, etc. A photograph taken in the hospital or office environment may inadvertently have a patient in the background.

29

Routine Vs. Non-Routine Disclosures

- For routine or recurring requests and disclosures, covered entities must implement reasonable policies and procedures (which may be standard protocols) to limit the information disclosed or requested.

30

Routine Vs. Non-Routine Disclosures

- For non-routine disclosures and requests, covered entities must develop reasonable criteria for determining and limiting the disclosure or request to the minimum necessary for the intended purpose, and review and limit each disclosure or request on an individual basis in accordance with these criteria. For certain disclosures, the Privacy Rule permits a covered entity to rely, if reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose, such as when the information is requested by another covered entity.

31

Responsibility for the Notice of Privacy

- The requirement for mandatory written consent has been revised under modifications to the standards. However, you still are required to provide notice to the patient regarding privacy rights and the privacy practices of the covered entity. You may also still develop a policy that requires consent. You are only **required** to make a good faith effort to obtain the patient's written acknowledgement of the receipt of the notice of privacy policy.

32

Responsibility for the Notice of Privacy

- Notice regarding your privacy guidelines and protocol practices must be posted in the office, and on your practice website if applicable. You must provide a copy of the notice to the patient. Notice should be provided prior to treatment, payment and healthcare operations unless there is an extenuating circumstances such as an emergency. In the case of emergency, the receipt of notice requirements could be delayed until practical.

33

Responsibility for the Notice of Privacy

- Even though a patient signature is not required it is preferred. Normally notice is only required if there is a Direct Treatment Relationship/Responsibility (DTR). For all non-treatment, payment, or healthcare operations a written authorization is required under the standards.

34

Responsibility for the Notice of Privacy

- Failure of the provider to obtain patient acknowledgement would not be a violation as long as there was a good faith effort. Dental providers should document all attempts at notification of the privacy notice.

35

Notice of Privacy

- Who can give authorization and acknowledge receipt of Privacy Notice:
- Patient – competent adult/emancipated minor
- Legal guardian or parent of minor
- Executor of estate, or individual appointed by probate court on behalf of deceased individual

36

Notice of Privacy

- In the case of incompetent, comatose, or critically ill individual to provide consent, the following legal representatives are able to sign consent:
  - Legal guardian or appointed attorney
  - Individual with Power of Attorney, individual named in advanced directive
  - Next of kin – spouse, adult child, father or mother, adult brother or sister

37

Parents as Representatives of Minors

- State or other applicable law governs in the area of minors. The privacy rule gives control of the minor's health information to the parent, guardian, or person acting in loco parentis unless state law supersedes, or the minor or some other representative is court authorized to control the health information and is legally able to consent to treatment.

38

Parents as Representatives of Minors

- Parents that agree to allow a confidential relationship between the physician and minor will also be excluded from receiving information. The regulation also denies disclosure to a parent if the covered entity determines disclosure would be harmful to the minor.

39

Patient Confidentiality Guidelines For Front Desk Staff

- All patients have the right to have confidential care provided. No one wants to receive services and have that information available and/or given to others without a right or need to know. It is your responsibility to protect this sensitive personal information. All information, medical or social, whether written, spoken, and electronic or computer generated is to be held in strict confidence.

40

Patient Confidentiality Guidelines For Front Desk Staff

- There is no reason or situation that would justify communication of this patient information, unless it is communicated to you on a need to know basis in order for you to do your job duties.

41

Patient Confidentiality Guidelines For Front Desk Staff

- Patient confidentiality begins from the moment you receive the first information in regards to this patient. This information could come from the patient, family member, dental professional, or other health care professional. Patient confidentiality continues after death in many cases.

42

Patient Confidentiality Guidelines For Front Desk Staff

- As an employee, you may be part of the information gathering cycle or you may only be exposed to the information. You are responsible for maintaining strict confidentiality without regard of how you came into possession of the information.

43

Patient Confidentiality Guidelines For Front Desk Staff

- Confidential information should not be discussed with anyone except on a professional need-to-know basis in order to further the delivery of patient care. Releasing confidential patient information, where intentional or accidental, is in conflict with the professional guidelines of any medical/healthcare entity. Violations in many hospitals and medical facilities should and will lead to disciplinary action, suspension, or even discharge.

44

Patient Confidentiality Guidelines For Front Desk Staff

- This is a risk management issue that should be and is taken extremely seriously by the dental health care team. Any time there is confidential patient information abuse there is potential for a lawsuit against not only the practice but also against the individual employee.

45

Patient Confidentiality Guidelines For Front Desk Staff

- Computer systems provide a fast means of storing and utilizing patient-related data, however, they also provide a potential for abuse of that data. You should:
  - Only access the information needed to perform your specific job duties.
  - Never access patient information on any patient that you are not directly involved with or have a need to know.

46

Patient Confidentiality Guidelines For Front Desk Staff

- Never share computer passwords or codes with others.
- Never leave your area and leave protected health information exposed.
- Never access patient information for other persons unless they are in a need to know position also.

47

Patient Confidentiality Guidelines For Front Desk Staff

- Sometimes you may hear or receive information about a friend or relative, or even friends or relatives of other employees or friends. You may see the dental chart or lab information, for example in your daily work. You will be tasked with keeping that information confidential also.

48

Patient Confidentiality Guidelines For Front Desk Staff

- If you are asked by co-workers or other staff for confidential information and it is not obvious why they needed the information, ask:
  - "In what regard do you need this information?"
  - "Why do you need this information?"
  - "Do you need it for your job?"

49

Patient Confidentiality Guidelines For Front Desk Staff

- If you are asked for information or asked for confirmation of confidential information by an individual that has no need to know, some helpful responses are:
  - "I'm sorry, I can't release that information."
  - "I'm not allowed to provide that confidential information."
  - "I've been asked not to release that information."
  - "Did you have a need for that information?"
  - "You will need to speak with the office manager, my supervisor, the dentist or the appropriate level person."

50

Patient Confidentiality Guidelines For Front Desk Staff

- If someone starts to provide you with information that is confidential you should answer:
  - "I have no need to know that information."
  - "How did you find that out? That should be confidential and not given out to anyone that does not have a need to know."

51

Patient Confidentiality Guidelines For Front Desk Staff

- You will sometimes have requests for information from outside sources. Your office/facility should have policies for handling such requests. In certain situations, passing on information is a violation of federal or state laws that could result in civil or criminal lawsuits.
- What happens if you fax medical records to the wrong recipient? See "Sample Medical Records Fax Transmission Authorization".

52

HIPAA Checklist for the Front Desk

- I need to:
  - Know who to direct HIPAA-related complaints and concerns to. (HIPAA Compliance and Security Office)
  - Evaluate computer (and networking) systems, both internally and externally. Document current processes and procedures in order to determine potential weak spots in the storage, manipulation, dissemination, transmission as well as disposal of PHI/IIHI.
  - Determine who or what entities I share information with, both in and outside of the office.

53

HIPAA Checklist for the Front Desk

- Evaluate protocol for delivery of the Notice of Privacy (NOP) and acknowledgment of receipt of NOP.
- Determine appropriate method for tracking patient PHI disclosure limitations as well as instances where the patient may revoke consent.
- Follow safeguards to protect PHI/IIHI from the administrative, technical levels as well as physical level.
- Know whom information can be released to and how to physically protect the information, ie. Physical records, oral communication, hard copy, or electronic etc., as well as e-mail, fax, electronic storage devices, etc., in and out of the office.

54

HIPAA Checklist for the Front Desk

- Evaluate the location of computers, phones, and faxes, including what can be seen, overheard, or received and not retrieved resulting in a breach.
- Evaluate how secure record maintenance storage is.
- Evaluate how all PHI/IIHI is destroyed.
- Ensure that no PHI is exposed on desks/counter, etc
- Begin now to make other staff aware of patient privacy issues such as what type of information is protected, who can they release information to, the actual process, etc.

55

HIPAA Checklist for the Front Desk

- Ensure that patient sign-in sheets, posted schedules, etc contain no PHI unless in authorized staff only area.
- Ensure that conversations are held in confidential tones of voice, ie phone, treatment areas, reception, checkout, collection, and discussion between other staff members.
- Ensure that no PHI is released over intercom.
- Ensure that chart pockets are PHI protected.
- Evaluate PHI flow through the front desk area and determine if non-authorized persons have access.

56

HIPAA Checklist for the Front Desk

- Follow established written policies on medical records with restrictions on disclosure.
- Know who has authorized access to PHI in order to release info.
- Always wear appropriate identification in the office.
- Never share passwords. If log-in procedures are already in place, audit and review. Never share passwords with other employees. If they have forgotten theirs, they will need a new one.

57

HIPAA Checklist for the Front Desk

- Review, revise, or initiate authorization forms for release of information for all purposes, not just treatment, payment, or healthcare operations (TPO).
- Inititate the Patient Notice of Information Use and Disclosure Form.
- Know the practice policy on patient right to view and obtain copies of the records, report of non-routine disclosures of PHI/IIHI and the patient's right to initiate corrections of inaccurate or incomplete information.

58

HIPAA Checklist for the Front Desk

- Attend the privacy training for all staff and sign the patient confidentiality statement.
- Know the reporting systems for the reporting of violations. What happened, who was involved, and how can it be prevented in the future?
- Develop a system to alert you when someone new, such as computer maintenance, software trainer, etc. will have access to PHI/IIHI. Do you have a Business Associate contract with them in which they agree to keep your information confidential?

59

HIPAA Checklist for the Front Desk

- Participate in a level of progressive discipline and re-training protocol for staff violating the practice privacy and security policy.
- Assess the physical arrangement of facility and equipment for potential areas of violation. Overhead conversations, visible computer screens, charts on desks, or in chart holders outside of treatment rooms, etc.
- Ensure that computers have been set up with virus protection.

60

HIPAA Checklist for the Front Desk

- Ensure that computers are logged off at the end of the day
- Ensure that records are secure at the end of the day.
- Ensure that computer passwords and login codes are personal, secret, and not shared.
- Know the contingency plan for data backup and disaster recovery.

61

Be Mindful….

- Stand where your patients check in and walk the paths your patients walk. Do you see any PHI (name, address, phone, e-mail, SS numbers, etc) anywhere on the desks, receptionist counters, computer monitors, or shelves? Remember, many people can read upside down and side-ways, so if it's visible, someone can read it!

62

Be Mindful….

- If you have any personal mobile devices connected to your office network, is all PHI encrypted?
  - It's now common practice for dentists, assistants, etc. to use the same mobile device for viewing and sending PHI as they do for making calls, downloading apps, and Internet browsing. What happens if a new app you download contains malware and logs every action your phone makes (including the PHI you viewed earlier that day?) If you must use a personal device at work, ensure the PHI you send or view is encrypted.

63

Resources

- www.cms.hhs.gov
  - Centers for Medicare and Medicaid Services website
- www.disa.org
  - Data Interchange Standards Association website
- www.nubc.org
  - This website contains standards for institutional claims
- www.nucc.org
  - This website contains information on non-institutional claim submission.

64

Any Questions?

???

65

- Contact: Rhonda@rhondagranja.com

Thank You!!

66