TSHA

TSHA Business Management Committee's Forum:

PREVENTING ETHICAL DELIMMAS

Panel: Lisa Milliken, M.A., CCC-SLP, FNAP
Melanie Johnston, M.A., SLP, CAS
Mendi Lancaster, MS, CCC-SLP, CBIS
Cathleen Lochte Swallows, MS, CCC-SLP
Amy Cantu, M.A., CCC-SLP, LSLS Cert. AVT
Stephanie O'Silas, MS , CCC-SLP
Erika Hayes - Student Representative

1

Preventing Ethical Dilemmas

2

Ethics and common related offenses

3

Business practice errors that impact ethics and reimbursement

- Billing for unskilled care
- Not following funding and payer guidelines
- Documentation compliance issues: timely documentation, SMART goals, legible notes, signatures, signed POC's within Medicare and license guidelines
- Students used inappropriately in therapy

4

Skilled Care

- Use expert knowledge for clinical decision-making
- Develop and modify treatment and maintenance programs
- Must be medically necessary
- Train and instruct others
- Analyze medical/behavioral data and select appropriate assessment tools to determine diagnosis and prognosis
- Develop/deliver therapy activities following hierarchy of complexity to achieve target skills for functional goal

5

Skilled Care

- Modify activities to maintain patient motivation and facilitate success (complexity of task; cueing; criteria for successful performance (accuracy, reps, response latency)
- Introduce new tasks to evaluate patient's ability to generalize skill
- Conduct ongoing assessment of progress to modify POC
- Explain rationale for treatment and expected results

6

Unskilled Care: Assistants, Qualified Personnel, Caretakers

- Perform activities as instructed
- Report observations and behaviors without interpretation, analysis or clinical judgment
- Report on activities without connecting performance to patient's goals

7

Documentation of skilled care:

- Describe skilled intervention
- Changes made to treatment due to assessment of patient's needs, patient's progress or regression
- Reason for lack of progress and justification for continued therapy if therapy will continue after plateau
- Indicate rationale (how service relates to functional goal), type, and complexity of activity
- Provide feedback about the performance including subjective changes (i.e. "He can now swallow without drooling.")
- Patient/caregiver's accuracy, frequency of performing activities

8

Example of Documentation of Skilled Care

- Patient performed tongue sweeps of buccal cavity with min cues on 80% of solid bolus trials to eliminate residue in mouth which puts patient at risk of aspirating the material.

9

Documentation of unskilled:

- Repetition of the same activities as in previous sessions with no notation of modifications, cueing level, or observations that would change plan of care
- Report on performance during activities with no description of modification, cueing level, feedback or caregiver training provided during the session
- Report on performance that reflects patient's skill level is static, with no notation of modifications to activities and cueing level

10

Example of Documentation of Unskilled Care

- Patient performed 10 reps of oral motor exercises.
- PO trials of thin liquid performed.
- Vitalstim used on placement 2b at 15 mAmps.

11

Other issues with documentation:

- Late notes
- Sloppy, disorganized notes with spelling errors or erroneous data: proofread!!
- Plan of cares are not signed in a timely manner and therefore there is no POC/signed order to support therapy
- Seeing patients for a different frequency than stated on the POC or longer than anticipated

12

Coding and billing errors

- Insurance verification and pre-authorization is essential
- Keep track of visits and charges to not mischarge, treat for longer than pre-cert approved, charge for codes not approved
- Pay attention to billing rules

13

Universal guidelines

- CCI edits: automated edit system to control CPT codes used on the same day (i.e. -59 modifier)
- Novitas: Texas MAC (Medicare Administrative Contractor) who regionally manage policies and payment related to reimbursement and act as the fiscal intermediary for Medicare
  - Local Coverage Articles: "rule books" or regional policy guidelines related to billing and coding
- CPT code revisions by the AMA

14

Examples of billing errors:

- Bill 92507 Speech Treatment more than once per day
- Bill 92507 Speech Treatment and 97129/97130 Cognitive Intervention on the same day
- Bill 96105 Assessment of Aphasia for non-standardized, informal assessment
- Bill 96125 Cognitive Performance Testing for SLUMS or MOCA
- Bill 92508 Speech Group for 8 patients working on language
- Bill 92508 Speech Group for 3 patients working on dysphagia

15

Resources for Rules/Guidelines

- https://www.asha.org/uploadedFiles/2020-Medicare-Physician-Fee-Schedule-SLP.pdf
- https://www.novitas-solutions.com/webcenter/portal/MedicareJH/pagebyid?contentId=00024343
- https://www.asha.org/Practice/reimbursement/coding/CCI-Edit-Tables-SLP/
- https://www.asha.org/practice/reimbursement/coding/SLPCPT/

16

DOCUMENTATION PITFALLS: LEAD TO DENIAL

17

Documentation is the KEY

- This is our only record of what we did and justification to be paid.
- It's essentially the invoice/ itemized statement to the payor who is reviewing it.
- We have to show thought process, progression, changes over time….

18

Common Denials

- Stagnant therapy that does not change in complexity: games or rote tasks
- Lacking objective data
- Goals not updated
- Unskilled care and services (maintenance therapy)
- Missing documentation
- Services not reasonable and necessary
- Incorrect ICD 10 coding or use of incorrect CPT codes

19

Students & Medicare

- To bill for interventions provided by ST students with Medicare patients, the student must be under direct supervision.
  - *The therapist is doing nothing else other guiding and directing the students care.*
  - The student may sign the note secondary with their student designation.
- The supervising clinician may not be treating any other patient during the time the student is treating a Medicare patient

20

Students & Non-Medicare

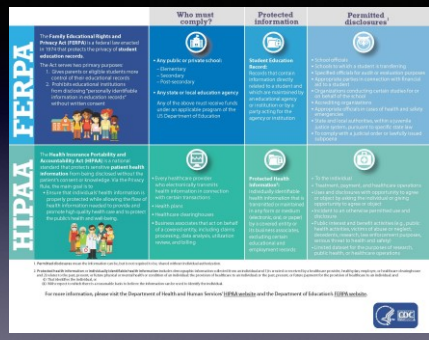
- Use guidelines for supervision by ASHA.
  - *The student must be supervised for >25% of the patient's direct care.*
  - *Supervision needs is dependent of the student's knowledge, competence and experience.*
  - *Supervisor is fully responsible for the care given by the student to the patient.*
  - The student may sign the note secondary with their student designation.

21

HIPAA & FERPA privacy rules

Amy Cantu, M.A., CCC-SLP, LSLS Cert. AVT

22



23

HIPAA Privacy Rule

- Establishes national standards to protect individuals' medical records and other protected health information (PHI)
- Outlines minimum Federal standards

24

HIPAA Privacy Rule

- Applies to
  - Covered Entities
    - Health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically
    - Hospitals, clinics, physicians, and other health care providers
  - Business associates hired by covered entities

25

HIPAA Privacy Rule

- Does not apply to the following entities that may have health information
  - Employers
  - State and local law enforcement
  - State agencies (e.g. CPS)
  - Schools and school districts
    - Health records protected by the Family and Educational Rights and Privacy Act (FERPA)

26

HIPAA Privacy Rule

- Requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.
- Gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

27

HIPAA Privacy Rule

- Major goal:
  - Properly protect an individual's health information **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.**
- Regulates who can have access to Protected Health Information (PHI), the circumstances in which it can be used, and who it can be disclosed to.
- Designed to be flexible and comprehensive

28

Individually Identifiable Health Information (PHI)

- Full name or last name and initial(s)
- Geographical identifiers smaller than a state
- Dates directly related to an individual, other than year
- Phone Numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers
- Device identifiers and serial numbers;
- Web Uniform Resource Locators (URLs)
- IP addresses
- Biometric identifiers, including finger, retinal and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

29

What are a patient's rights regarding PHI?

1. The right to receive a notice about your privacy policies.
2. The right to access the medical information you maintain about him or her.
3. The right to limit the uses and disclosure of medical information.
4. The right to request amendments to the medical record.
5. The right to revoke or limit authorization.
6. The right to an accounting of disclosures of PHI.

30

Permitted Uses and Disclosures

- A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:
  - (1) To the Individual (unless required for access or accounting of disclosures);
  - (2) Treatment, Payment, and Health Care Operations;
  - (3) Opportunity to Agree or Object;
  - (4) Incident to an otherwise permitted use and disclosure;
  - (5) Public Interest and Benefit Activities; and
  - (6) Limited Data Set for the purposes of research, public health or health care operations.
- Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

31

Uses and Disclosures for Treatment, Payment, and Health Care Operations

- "Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

Data from Section 164.506 [45 CFR 164.506]

32

Huh?

- HIPAA should not restrict treatment of a patient
- Sharing of information between providers can happen without patient "consent"

33

- Do you need consent to discuss the patient's performance with others in your organization who are directly treating the patient?
  - No. A covered entity may use protected health information about an individual to provide health care to the individual and may consult with other health care providers about the individual's treatment.
- Do you need consent to discuss the student's test results with their teacher?
  - No. The Privacy Rule allows health care providers that are covered entities to use or disclose protected health information, such as X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes without the patient's authorization. This includes sharing the information to consult with other providers, including providers who are not covered entities, to treat a different patient, or to refer the patient. (including providers not covered by the Privacy Rule)*

34

- Do you need consent to send a patient's record to a specialist who needs the information to treat the individual?
  - No. A covered entity may disclose protected health information for the treatment activities of any health care provider (including providers not covered by the Privacy Rule)
- Can health care providers, such as a specialist or hospital, to whom a patient is referred for the first time, use protected health information to set up appointments or schedule surgery or other procedures without the patient's written consent?
  - Yes. The HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.

35

- Are health care providers restricted from consulting with other providers about a patient's condition without the patient's written authorization?
  - No. Consulting with another health care provider about a patient is within the HIPAA Privacy Rule's definition of "treatment" and, therefore, is permissible. In addition, a health care provider (or other covered entity) is expressly permitted to disclose protected health information about an individual to a health care provider for that provider's treatment of the individual.
- Does a physician need a patient's written authorization to send a copy of the patient's medical record to a specialist or other health care provider who will treat the patient?
  - No. The HIPAA Privacy Rule permits a health care provider to disclose protected health information about an individual, without the individual's authorization, to another health care provider for that provider's treatment of the individual.

36

Can Information Be Shared Freely When It Relates to a Patient?

- No.
- Covered entities can only share information without consent when all 3 requirements are met:
  1. Both CEs must have or have had a relationship with the patient (can be a past or present patient)
  2. The PHI requested must pertain to the relationship
  3. The discloser must disclose only the minimum information necessary for the health care operation at hand.
- HIPAA privacy rule depends on covered entities using their best judgement when deciding what information to disclose without consent

37

Sharing Information without Consent

- I'm still unsure…
  - Get consent

38

What is the difference between "consent" and "authorization"

- Consent
  - Voluntary
  - Only for "uses and disclosures of protected health information for treatment, payment, and health care operations"
- Authorization
  - Required by the HIPAA privacy rule
  - For PHI uses and disclosures not otherwise allowed by the rule
  - Voluntary consent is not sufficient
  - Detailed document that gives the covered entity permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

39

What is the difference between "consent" and "authorization"

- Authorization cont.
  - must specify a number of elements, including a description of the protected health information to be used and disclosed
  - the person authorized to make the use or disclosure
  - the person to whom the covered entity may make the disclosure
  - an expiration date
  - in some cases, the purpose for which the information may be used or disclosed.
  - With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.

40

Family Educational Rights and Privacy Act (FERPA)

- Federal law that protects the privacy of student education records.
- The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education
- The Act serves two primary purposes:
  1) Gives parents or eligible students more control of their educational records
  2) Prohibits educational institutions from disclosing "personally identifiable information in education records" without written consent

41

Health Records vs. Education Records

- The HIPAA Privacy Rule generally does not apply to primary and secondary schools (K-12).
- A student's health records are defined as education records.
- Includes:
  - Immunizations
  - Records obtained by a school nurse
  - Records on services provided to students under the Individuals with Disabilities Education Act (IDEA)

42

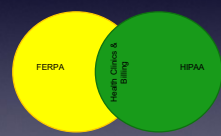
FERPA Permitted Disclosures

- Schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
  - School officials with legitimate educational interest
  - Other schools to which a student is transferring
  - Specified officials for audit or evaluation purposes
  - Appropriate parties in connection with financial aid to a student
  - Organizations conducting certain studies for or on behalf of the school
  - Accrediting organizations
  - To comply with a judicial order or lawfully issued subpoena
  - Appropriate officials in cases of health and safety emergencies
  - State and local authorities, within a juvenile justice system, pursuant to specific State law.

43

Where do FERPA and HIPAA Intersect?

1. When a school provides health care to students in the normal course of business (health clinic)
2. When a school conducts any covered transactions electronically in connection with health care provided in #1



44

Does FERPA apply to school student health records maintained by a health care provider that is not employed by a school?

- If the entity is acting on behalf of a school and maintaining student health records, these records are considered education records under FERPA
- If the entity is an outside party who is providing services directly to the student and is not employed by the school nor are they acting on behalf of the school, then these records are not considered "education records" and are not subject to FERPA (even if the services are provided on school grounds)
  - In these situations, the school must obtain parental consent in order to provide information to this entity

45

Can a health care provider disclose PHI about a student to a school nurse or physician?

- Yes. The HIPAA Privacy Rule allows covered health care providers to disclose PHI about students to school nurses, physicians, or other health care providers for treatment purposes, without the authorization of the student or student's parent

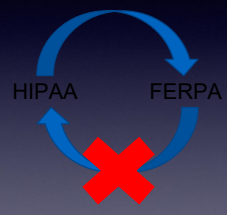
46

Under what circumstances does FERPA permit an eligible student's treatment records to be disclosed to a third-party health care provider for treatment?

- An eligible student's treatment records may be shared with health care professionals who are providing treatment to the student, including health care professionals who are not part of or not acting on behalf of the educational institution (i.e., third-party health care provider), as long as the information is being disclosed only for the purpose of providing treatment to the student.
- Education Records and Treatment Records are not the same thing

47

The flow of information…



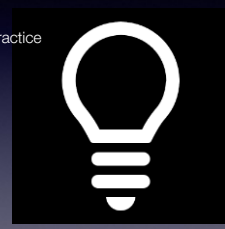
48

Overview: ASHA Code of Ethics

49

Reflect: *what we DO know…*

- The Code of Ethics—our "standard" of practice
- -Defines our professional role and responsibilities
- -Guides our professional conduct
- -Developed by the American Speech-Language Hearing Association (ASHA)
- Published on ASHA's website for easy access

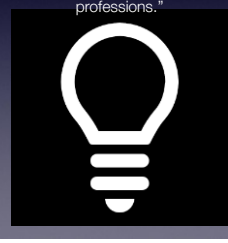


https://www.asha.org/Code-of-Ethics/#sec1.2

50

Reflect: *what we DO know…*

"The ASHA Code of Ethics is intended to ensure the welfare of the consumer and to protect the reputation and integrity of the professions."



51

Legal Implications

- The Code of Ethics influences state professional practice laws.
- The ASHA Code of Ethics was not developed by TDLR but *informs* state law about reasonable expectations for our role, qualifications, responsibilities, and professional conduct.
- Unprofessional conduct as specified in the code of ethics adopted and published by The Texas Commission of Licensing and Regulation and the Texas Department of Licensing and Regulation is subject to disciplinary action when a violation occurs.
- "By holding ASHA certification or membership, or through application for such, all individuals are automatically subject to the jurisdiction the ASHA Board of Ethics for ethics complaint adjudication."

52

The Primary Four *Principles of Ethics*:

- Outlines our ***responsibilities and obligations*** to our profession
- Encompasses several "rules" pertaining to the overarching principle
- "The Rules of Ethics are specific statements of minimally acceptable as well as unacceptable professional conduct."

53

The Primary Four *Principles of Ethics*:

Remember RESPONSIBILTY…

1. to persons served professionally and to research participants, both human and animal
2. for one's professional competence
3. to the public
4. for professional relationships

54

Principles of Ethics:

Considerations for Principle 1 of 4

"Individuals shall honor their responsibility to hold paramount the welfare of persons they serve professionally or who are participants in research and scholarly activities, and they shall treat animals involved in research in a humane manner."

Protect Confidentiality

Timely Documentation

Informed Consent

Non-Discrimination

Non-Misrepresentation of Credentials

Delegating with responsibility to patient welfare

Using independent and evidence-based clinical judgement

Competence!!

Non-coercion

Quality/Outcome Tracking

55

Principles of Ethics:

Considerations for Principle 1 of 4

Reflection 1: Competence

What does it look like to document competencies for the private practitioner or group practice?

Reflection 2: Evaluating effectiveness of services (quality)

How are you currently documenting the effectiveness of your services? What do you require of yourself or from your staff?

Reflection 3: "use every resource, including referral and/or interprofessional collaboration when appropriate, to ensure that quality service is provided"

How do you know when a client needs a certain therapy provider? In what ways can you support a referral?

56

Principles of Ethics:

Considerations for Principle 1 of 4

Reflection 1: Competence

Maintain records of CEUs, Skills Checklists

Reflection 2: Evaluating effectiveness of services (quality)

Daily/Progress Reports with measurable Baseline/Current %
Quality Indicators (e.g. BIMS)
Functional Outcome Measures (ASHA NOMS)

57

Principles of Ethics:

Considerations for Principle 1 of 4

Reflection 3: "use every resource, including referral and/or interprofessional collaboration when appropriate, to ensure that quality service is provided"

Be familiar with the work of other disciplines (e.g. OT is indicated for upper/lower body dressing, bed mobility, grooming/eating, etc.).

Are you aware of signs/symptoms that would indicate a certain intervention? (e.g. ABA, PsyD, social worker etc.).

Networking amongst interdisciplinary colleagues at work or in the community can improve referral network and awareness about what others can do for our patients

58

Principles of Ethics:

Considerations for Principle 2 of 4

"Individuals shall honor their responsibility to achieve and maintain the highest level of professional competence and performance."

Common themes found in the Rules:

-Engage only in your scope of practice
-Researcher compliance standards
-Enhance and refine professional competence
-Defines individuals qualified to provide services
-Use technology/instruments consistent with professional guidelines
-Ensure tools/instruments are calibrated correctly

59

Principles of Ethics:

Considerations for Principle 3 of 4

"Individuals shall honor their responsibility to the public when advocating for the unmet communication and swallowing needs of the public and shall provide accurate information involving any aspect of the professions."

Common themes found in the Rules:

"Honesty and without omission"

Avoid conflicts of interest

Zero tolerance for fraud and negligence
Avoid Misrepresentation
Accurate and complete Public Relations (PR)

60

Principles of Ethics:

Considerations for Principle 4 of 4

"Individuals shall uphold the dignity and autonomy of the professions, maintain collaborative and harmonious interprofessional and intraprofessional relationships, and accept the professions' self-imposed standards."

Common themes found in the Rules:

Patient-centered collaboration

Integrous practice

Responsibility to report violations

Behavioral conduct with colleagues

Behavioral conduct with clients served

Appropriate research conduct

Due Diligence

61

Staying Compliant

Large and small organizations are encouraged to include a review of the ASHA Code of Ethics with SLP staff periodically to avoid punishable offenses

It is useful and meaningful to discuss scenarios that are exemplary of compliance and non-compliance—let's not assume that everyone knows!

Common Violations
(found punishable by TDLR)

- Respondent has been convicted of an offense that directly relates to the duties and responsibilities of the licensed occupation.
- Respondent failed to properly maintain and secure records for each client or initial consultation.
- Respondent failed to maintain accurate records of professional services rendered.

62

Staying Compliant—Avoid Common Violations

- Respondent failed to provide services as specified in treatment plans.
- Respondent falsified client therapy notes by forging a caregiver's signature resulting in billing for services not actually rendered.
- Respondent failed to verify that the duties of an intern or assistant were appropriate.

Respondent has been convicted of a crime involving fraud or deceptive trade practices; Respondent lacks sufficient honesty, trustworthiness and integrity to hold a license.

Respondent falsified record of speech language pathology services and received payment for services based off the falsified records.

Respondent falsified client treatment records resulting in billing for services not actually rendered.

63

HB 300

- Privacy compliance measure mandated by state law in Texas (Texas House Bill 300)
- Provides a security rule that focuses on administrative, technical, and physical safeguards specific to electronic PHI.
- Violations of HB 300 are subject to penalties and sanctions including hefty monetary fines, loss of licensure and accreditation, and jail time for willful, criminal offenses.

64

HB 300

Mandates that healthcare providers take highest measure to secure patient electronic data.

- The Security Rule permits sending PHI with email, but only if the email and its PHI are protected with encryption
- Example: if you decide not to encrypt, and there is a data breach, you/your company can be held fully liable and subject to fines. However, if you DO encrypt and there is a data breach, then you/your company would not be liable because every possible precaution to protect data was performed.

65

HB 300

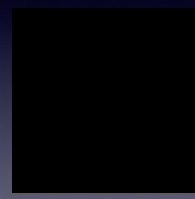
Large and small healthcare companies can ensure compliance by:

- Adopting clear privacy and security policies and procedures for the owner and employees to follow
- Train employees on HIPAA and HB 300 and on HIPAA-related policies and procedures on hire and every year.
- Secure patient records so that they are protected from misuse or inappropriate disclosure.

66

HB 300 — Compliant or Non-Compliant?

- Utilizing a secure fax with a BAA in place
- Utilizing an encrypted email
- Utilizing a business associate agreement for online fax and other email/voice communication systems
- Not providing a record release and electronic disclosure form to patients before releasing medical records
- Adjusting settings in your EMR to limit access/view of medical records to providers not directly involved in a patient's case



67

Ethical Decision-making Tools

68

Violations of HIPAA and Client Confidentiality

Social Media and other costly mistakes

69

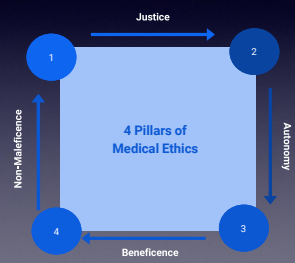
Communication in the Electronic Age

70

Ethical Decision-making Tools

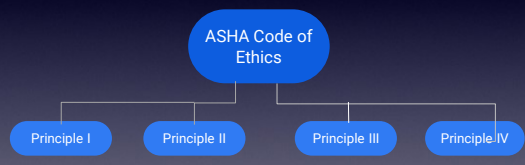
71

Ethical Decision-Making Tools



72

ASHA CODE OF ETHICS



73

Texas Code of Ethics

- **Subchapter J**
  - License denial and disciplinary procedures
  - Section 401.451 Grounds for License Denial and Disciplinary Action
  - https://www.tdlr.texas.gov/slpa/slpalaw.htm#401.451
- **Subchapter P**
  - Responsibilities of the licensee and code of ethics
    - Separated into "Licensee Shall:" and a "Licensee Shall Not"
    - More specific than ASHA Code of Ethics
    - https://www.tdlr.texas.gov/slpa/slparules.htm#111155

74

Ethics Resources

1	ASHA Code of Ethics	• ASHA Ethics Resources • Everyday Ethical Blog • Complaint filing process • Ethics for specific areas of practice • Ethics Education • https://www.asha.org/practice/ethics/
2	Texas Code of Ethics	• TDLR • Texas Code of Ethics • Complaint filing process • https://www.tdlr.texas.gov/slpa/slpa.htm

75

Ethical Use of Social Media

- HIPAA / Research Violations
  - Principle I
    - Rule O
    - Rule P
- Misrepresentation of Services / Experience / Advertising / Credentials
  - Principle I
    - Rule D
  - Principle III
    - Rule A
  - Principle IV
    - Rule C

76

Violations of HIPAA and Client Confidentiality

Social Media and other costly mistakes

77

What is HIPAA?

- The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that:
  - Protects the privacy of patient health information
  - Provides for the electronic and physical security of patient health information
  - Prevents healthcare fraud and abuse
  - Simplifies billing and other transactions, reducing health care administrative costs
  - Gives patients rights over use and disclosure of their health information
- HIPAA Privacy Rule:
  - Sets standards on maintaining the privacy of Protected Health Information (PHI)
- HIPAA Security Rule:
  - Requires the security of electronic forms of PHI, or e-PHI
  - Defines the standards to implement safeguards to protect e-PHI

78

Updates to the HIPAA Law

The HITECH Act updated HIPAA in 2009
- Notification requirements in event of a breach
- Fines and penalties increased for privacy violations
- Right to request copies of the electronic health care record in electronic format
- Mandates that Business Associates have civil and criminal liability for privacy and security violations

- Additional changes to HITECH published January 2013
  - Broader definition of a "breach" of unsecured PHI
  - Increased duties on Business Associates, as well as subcontractors of Business Associates

79

What Information Must Be Protected?

- PHI is information related to a patient's past, present or future physical &/or mental health or condition
- PHI can be in any form: written/paper:
  - Soft charts
  - Spoken/oral (hallway discussion, voicemail)
  - Electronic (e.g., email, text, therapy software)
- PHI is any health information with identifiers
  - With at least 1 of 18 personal identifiers in of health information

80

PHI Identifiers

- Name
- Address
- All elements (except years) of dates related to an individual
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license #
- Any vehicle or device serial #
- Web URL
- IP Address
- Finger or voice print
- Photographic images
- Any other characteristic that could uniquely identify the individual

81

Patient Rights Under HIPAA

- Right to access their own medical records
- Right to request to amend or correct their records
- Right to an accounting of PHI disclosures
- Right to request a restriction limiting access by others to their records
- Right to request confidential communications of their health information
- Right to file a complaint if they believe their privacy rights have been violated

82

Keeping Health Information Secure is Part of Your Job

- Secure Faxing
- Safe Emailing
- No texting of PHI
- Safe Internet use
- Password Protection
- Conversations
- Therapy Department Security
- Social Media
- Discarding Papers
- Computer Security
- Know where you left your paperwork
- Removal of records
- Storage of records
- Building Access
- Verification of Requests
- Sharing PHI
- Disclosure of PHI

83

Common Ethical Issue: Confidentiality

- Records management, storage, ownership, retention
- Information exchanged
- Disclosure/release of information
- Access to records
- Exchange of records between professionals

84

Example HIPAA Violation

Recently, a Department of Health and Human Services Administrative Law Judge ruled in favor of the Office of Civil Rights (OCR) and required a Texas cancer center to pay $4.3 million in penalties for HIPAA violations.

- Failure to mitigate known security risk vulnerabilities
- Use of unencrypted thumb drives and laptops

OCR is serious about protecting health information privacy and they will pursue litigation.

85

Dermatology Practice Penalized for HIPAA Violations

- Private practices are the kind of covered entity most scrutinized by the Office of Civil Rights (OCR)
- In one HIPAA violation case, a dermatology practice lost an unencrypted flash drive that contained protected health information
- The group was fined $150,000 and was required to install a corrective action plan

86

HIPAA Violation Case : Submitting Bills to Collections

- Patient privacy advocate Dr. Barry Helfmann was president-elect of the ***American Group Psychotherapy Association***.
- According to case files, Dr. Helfmann's employees regularly forwarded past due patient bills to a collections firm.
- The bills contained protected info like CPT codes, which can reveal patient diagnoses.
- As a result, the State of New Jersey sought to suspend and revoke Helfmann's license.

87

Hospital Worker Charged with HIPAA Violation

- In 2014, Texas hospital employee Joshua Hippler got an 18-month jail term for wrongful disclosure of private patient medical information
- He was arrested in Georgia and found to be in possession of medical records
- Though the filing didn't say how many records he had, he was charged with wrongful disclosure of private health information for personal gain

88

Case Against Walgreen Pharmacist Leads to $1.4 Million HIPAA Award

- In 2014, a Walgreen Co. pharmacist violated the HIPAA act when she shared confidential medical info about a customer who once dated her husband.
- The customer's lawyer, Neal F. Eggeson Jr., said the case sets an example, since it proves businesses can now be held liable for the actions of their employees.

89

Criminal HIPAA Conviction for Respiratory Therapist

- Jamie Knapp, an employee of ProMedica Bay Park Hospital in Ohio, accessed 596 medical records in a 10-month period.
- Knapp was authorized to view records as part of her job, but only for the patients she was treating.
- Allegedly, she viewed files for unrelated patients. Knapp was convicted on criminal HIPAA violations by a federal jury in Ohio, facing up to one year in prison.

90

$2.5 Million Settlement in Stolen Laptop HIPAA Case

- A cardiac monitoring vendor got into HIPAA hot water when a laptop containing hundreds of patient medical records was stolen from a parked car.
- The OCR reached a $2.5 million settlement with the vendor, demonstrating that the federal government is extremely aggressive in prosecuting HIPAA cases involving third parties and portable digital media.

91

Facebook HIPAA Violation

- In 2017, a HIPAA violation resulted in the firing of a medical employee after she posted about a patient on Facebook.
- The 24 year old med tech commented on a post about a patient killed in a car crash, using the words, "Should have worn her seatbelt…"
- While the comment itself seems innocent and even public-minded, it disclosed PHI about the patient.
- The employee later told reporters she was fired for a HIPAA violation, though the hospital declined to comment.

92

Communication in the Electronic Age

93

The Risks Are Evident

- A healthcare provider who posts work-related information online could "unwittingly become ensnared in a disciplinary investigation at work, a federal investigation of a possible HIPAA violation, a disciplinary investigation by the state licensing board, and a civil lawsuit filed by an aggrieved patient."

Hader, Amy L.; Brown, Evan D. (2010)

94

95

The Internet is an Electronic Billboard

- You may expect electronic messages to remain private, but once you send it or post it you've lost all control over it
- Deleting an electronic message does not make it invisible or undiscoverable

96

No Social Media

- Do not post patient-related or sensitive information on a website or social networking site
- No Exceptions
- No Excuses

97

Utilizing Texting

When is texting appropriate at work?

- If your message is urgent or short & sweet:
  - "Call Me"
  - Say "I just sent you an email and I need a response"
  - Logistical communications: travel information, dates, times, locations of meetings are ok (if no names)

98

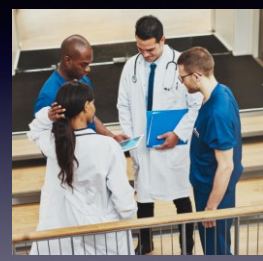
Make Voice Mail Better

- Don't leave detailed voice mails unless absolutely necessary
- Never leave substantive patient related messages on unfamiliar phone numbers
- Do not use a speaker phone unless privacy is assured
- Don't forget that voice mails are easily forwarded, passed along and otherwise shared.

99

Best Practices For Voice Communication

- Do not give PHI over the phone unless you confirm the identity of the listener & their authority to receive PHI
- Be aware of your surroundings and who is around to hear any discussions concerning PHI
- Refrain from discussing PHI in public areas such as coffee shops, airports, elevators, rest rooms, and reception areas

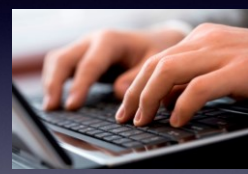


https://www.medisafe.com/blog/7-most-common-hipaa-violations-that-can-cost-your-practice

100

Recommendations for E-Mail

- E-mail PHI only to a known party (e g , patient, health care provider)
- Do not e-mail PHI to a group distribution list unless individuals have consented to such method of communication
- In the subject heading, do not use patient names, identifiers or other specifics; consider the use of a "confidential" subject line



101

Legal Implications of Email

- Healthcare is a highly regulated business and audits are common
- It is common for enforcement authorities (HHS, EEOC, FBI. OIG) to seek emails and text messages in discovery
- E-mail is a form of evidence and can be admitted as evidence in court in the same way as can other forms of documentary evidence

https://www.webdomus.net/box-cose-come-funziona-cloud-computing/

102

Message Tracking

- Emails have electronic 'metadata,' providing technical information about the drafting, alteration, timing, sending, receipt & even blind copy recipients of the email
- Even if files are overwritten, fragments of the documents survive, sometimes in several places on a computer
- Emails can be recovered from hard drives, servers, cloud storage, smart phones, internet service providers and any other media where electronic data is stored – even when information has been "deleted"

https://www.groovypost.com/howto/recover-data-non-booting-hard-drive/

103

Best Practices for Faxing

- Limit the PHI in the fax to the minimum
- Do not fax sensitive PHI (E.g., alcohol abuse, drug abuse, mental health issues, HIV testing)
- Take reasonable precautions to ensure the intended recipient is at the receiving machine
- If there is any question of the fax number accuracy, contact the recipient to confirm
- If you send a fax with PHI in error – you must notify your supervisor or Privacy Officer
- Call to confirm receipt
- Do not include any PHI on the fax cover sheet
- Remove sent faxes from machines

104

Communication Summary

- Keep your emails brief
- Know your audience
- Proof-read your emails
- Avoid sending unnecessary attachments
- Respond to emails swiftly
- Stop and think before you press 'Send'
- Don't pass along junk mail
- Blind copy with care
- Don't click on links or attachments in emails from unknown sources

105

Create a Culture of Ethical Practice in Communications

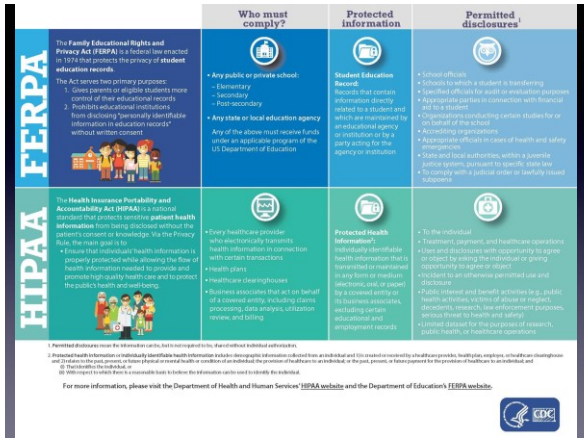
- Consistently communicate expectations of protecting patients' PHI
- Implement, and enforce privacy and security policies and procedures
- Keep health information confidential
- Incorporate and regularly re-evaluate:
  - Physical, technical, and administrative measures to protect patients' health records
  - Internal and external security threats
  - Assessment of and preparations for security risks in hardware/software, facility, and environment

106

HIPPA & FERPA Privacy Rules

Amy Cantu, M.A., CCC-SLP, LSLS Cert. AVT

107



108

HIPAA Privacy Rule

- Establishes national standards to protect individuals' medical records and other protected health information (PHI)
- Outlines minimum Federal standards

109

HIPAA Privacy Rule

- Applies to
  - Covered Entities
    - Health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically
    - Hospitals, clinics, physicians, and other health care providers
  - Business associates hired by covered entities

110

HIPAA Privacy Rule

- Does not apply to the following entities that may have health information
  - Employers
  - State and local law enforcement
  - State agencies (e.g. CPS)
  - Schools and school districts
    - Health records protected by the Family and Educational Rights and Privacy Act (FERPA)

111

HIPAA Privacy Rule

- Requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.
- Gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

112

HIPAA Privacy Rule

- Major goal:
  - Properly protect an individual's health information **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.**
- Regulates who can have access to Protected Health Information (PHI), the circumstances in which it can be used, and who it can be disclosed to.
- Designed to be flexible and comprehensive

113

Individually Identifiable Health Information (PHI)

- Full name or last name and initial(s)
- Geographical identifiers smaller than a state
- Dates directly related to an individual, other than year
- Phone Numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers
- Device identifiers and serial numbers;
- Web Uniform Resource Locators (URLs)
- IP addresses
- Biometric identifiers, including finger, retinal and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

114

What are a patient's rights regarding PHI?

1. The right to receive a notice about your privacy policies.
2. The right to access the medical information you maintain about him or her.
3. The right to limit the uses and disclosure of medical information.
4. The right to request amendments to the medical record.
5. The right to revoke or limit authorization.
6. The right to an accounting of disclosures of PHI.

115

Permitted Uses and Disclosures

- A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:
  - (1) To the Individual (unless required for access or accounting of disclosures);
  - (2) Treatment, Payment, and Health Care Operations;
  - (3) Opportunity to Agree or Object;
  - (4) Incident to an otherwise permitted use and disclosure;
  - (5) Public Interest and Benefit Activities; and
  - (6) Limited Data Set for the purposes of research, public health or health care operations.
- Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

116

Uses and Disclosures for Treatment, Payment, and Health Care Operations

- "Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

Data from Section 164.506 [45 CFR 164.506]

117

Huh?

- HIPAA should not restrict treatment of a patient
- Sharing of information between providers can happen without patient "consent"

118

- Do you need consent to discuss the patient's performance with others in your organization who are directly treating the patient?
  - No. A covered entity may use protected health information about an individual to provide health care to the individual and may consult with other health care providers about the individual's treatment.
- Do you need consent to discuss the student's test results with their teacher?
  - No. The Privacy Rule allows health care providers that are covered entities to use or disclose protected health information, such as X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes without the patient's authorization. This includes sharing the information to consult with other providers, including providers who are not covered entities, to treat a different patient, or to refer the patient. (including providers not covered by the Privacy Rule)*

119

- Do you need consent to send a patient's record to a specialist who needs the information to treat the individual?
  - No. A covered entity may disclose protected health information for the treatment activities of any health care provider (including providers not covered by the Privacy Rule)
- Can health care providers, such as a specialist or hospital, to whom a patient is referred for the first time, use protected health information to set up appointments or schedule surgery or other procedures without the patient's written consent?
  - Yes. The HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.

120

- Are health care providers restricted from consulting with other providers about a patient's condition without the patient's written authorization?
  - No. Consulting with another health care provider about a patient is within the HIPAA Privacy Rule's definition of "treatment" and, therefore, is permissible. In addition, a health care provider (or other covered entity) is expressly permitted to disclose protected health information about an individual to a health care provider for that provider's treatment of the individual.
- Does a physician need a patient's written authorization to send a copy of the patient's medical record to a specialist or other health care provider who will treat the patient?
  - No. The HIPAA Privacy Rule permits a health care provider to disclose protected health information about an individual, without the individual's authorization, to another health care provider for that provider's treatment of the individual.

121

Can Information Be Shared Freely When It Relates to a Patient?

- No.
- Covered entities can only share information without consent when all 3 requirements are met:
  1. Both CEs must have or have had a relationship with the patient (can be a past or present patient)
  2. The PHI requested must pertain to the relationship
  3. The discloser must disclose only the minimum information necessary for the health care operation at hand.
- HIPAA privacy rule depends on covered entities using their best judgement when deciding what information to disclose without consent

122

Sharing Information without Consent

- I'm still unsure…
  - Get consent

123

What is the difference between "consent" and "authorization"

- Consent
  - Voluntary
  - Only for "uses and disclosures of protected health information for treatment, payment, and health care operations"
- Authorization
  - Required by the HIPAA privacy rule
  - For PHI uses and disclosures not otherwise allowed by the rule
  - Voluntary consent is not sufficient
  - Detailed document that gives the covered entity permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

124

What is the difference between "consent" and "authorization"

- Authorization cont.
  - must specify a number of elements, including a description of the protected health information to be used and disclosed
  - the person authorized to make the use or disclosure
  - the person to whom the covered entity may make the disclosure
  - an expiration date
  - in some cases, the purpose for which the information may be used or disclosed.
  - With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.

125

Family Educational Rights and Privacy Act (FERPA)

- Federal law that protects the privacy of student education records.
- The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education
- The Act serves two primary purposes:
  1) Gives parents or eligible students more control of their educational records
  2) Prohibits educational institutions from disclosing "personally identifiable information in education records" without written consent

126

Health Records vs. Education Records

- The HIPAA Privacy Rule generally does not apply to primary and secondary schools (K-12).
- A student's health records are defined as education records.
- Includes:
  - Immunizations
  - Records obtained by a school nurse
  - Records on services provided to students under the Individuals with Disabilities Education Act (IDEA)

127

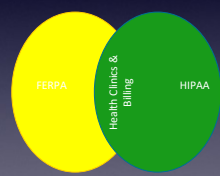
FERPA Permitted Disclosures

- Schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
  - School officials with legitimate educational interest
  - Other schools to which a student is transferring
  - Specified officials for audit or evaluation purposes
  - Appropriate parties in connection with financial aid to a student
  - Organizations conducting certain studies for or on behalf of the school
  - Accrediting organizations
  - To comply with a judicial order or lawfully issued subpoena
  - Appropriate officials in cases of health and safety emergencies
  - State and local authorities, within a juvenile justice system, pursuant to specific State law.

128

Where do FERPA and HIPAA Intersect?

1. When a school provides health care to students in the normal course of business (health clinic)
2. When a school conducts any covered transactions electronically in connection with health care provided in #1



129

Does FERPA apply to school student health records maintained by a health care provider that is not employed by a school?

- If the entity is acting on behalf of a school and maintaining student health records, these records are considered education records under FERPA
- If the entity is an outside party who is providing services directly to the student and is not employed by the school nor are they acting on behalf of the school, then these records are not considered "education records" and are not subject to FERPA (even if the services are provided on school grounds)
  - In these situations, the school must obtain parental consent in order to provide information to this entity

130

Can a health care provider disclose PHI about a student to a school nurse or physician?

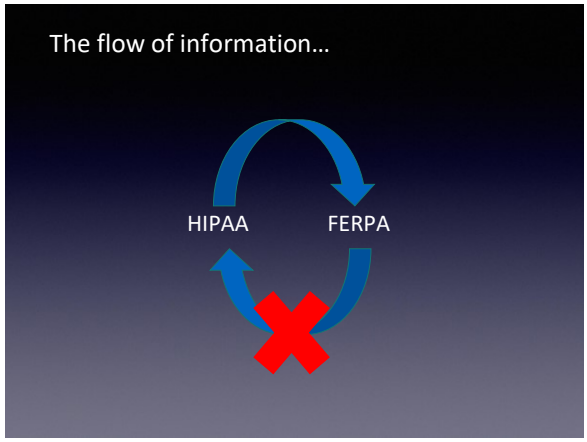
- Yes. The HIPAA Privacy Rule allows covered health care providers to disclose PHI about students to school nurses, physicians, or other health care providers for treatment purposes, without the authorization of the student or student's parent

131

Under what circumstances does FERPA permit an eligible student's treatment records to be disclosed to a third-party health care provider for treatment?

- An eligible student's treatment records may be shared with health care professionals who are providing treatment to the student, including health care professionals who are not part of or not acting on behalf of the educational institution (i.e., third-party health care provider), as long as the information is being disclosed only for the purpose of providing treatment to the student.
- Education Records and Treatment Records are not the same thing

132



133