Managing the Regulatory Environment

ADA's Guidelines for Practice Success™ (GPS™)

ADA Tip Sheet on Certain Provisions of the HIPAA Privacy Rule

The Privacy Rule establishes permitted and required uses and disclosures of protected health information (PHI), requires covered entities to take specific steps to safeguard PHI, and grants individuals certain rights, such as the right to inspect and obtain copies of their protected health information (PHI) maintained by or for a covered entity in either paper or electronic form in one or more Designated Record Sets (DRS). Additional information about the Privacy rule is available from the Department of Health and Human Services' (HHS) in Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524.

- ☐ The Privacy Rule applies to patients' PHI in all formats, such as:
  - ✓ paper
  - ✓ oral
  - ✓ electronic

    - PHI includes "individually identifiable health information" held or transmitted by a covered entity (CE) or its business associate (BA), in any form or media."
      - "individually identifiable" means that the data either identifies an individual or that there is a reasonable basis to believe the information can be used to identify an individual. Examples of identifiers that can make health information "individually identifiable" include a person's name, address, birth date, or Social Security number.
      - "health information" relates to an individual's past, present or future physical/mental health or condition, the provision of health care to the individual, or payment for the provision of health care.
      - covered entities (CE) include certain healthcare providers, healthcare clearinghouses, and certain insurers and health plans. CEs must follow HIPAA regulations
      - business associates (BA) provide services to, or perform functions or activities on behalf of, a CE involving individually identifiable health information. BAs must follow HIPAA regulations

    - Some Privacy Rule provisions apply to all PHI, and others apply only to "Designated Record Sets." A Designated Record Set (DRS) in a covered dental practice is a:
      - group of records maintained by or for a CE that is:
        - the medical records and billing records about individuals maintained by or for the dental practice, or
        - used, in whole or in part, by or for the covered entity to make decisions about individuals
        - For purpose of this definition, "records" are defined as being any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a CE
      - examples of records that might be DRS include:
        - electronic health records (EHR) and paper medical record
        - other medical, billing, payment, enrollment, claims records
        - clinical laboratory test reports
        - X-rays and other images

- wellness and disease management program information
- clinical case notes
- old/archived PHI

☐ The Privacy Rule applies to both internal uses and external disclosures of PHI:
- ✓ the use of patients' PHI internally within the covered entity or how PHI is shared within the entity that maintains the information
- ✓ the disclosure or external release, transfer, provision of access to, or divulging of patients' protected health information in any manner to anyone outside of the entity that maintains the information

☐ The Privacy Rule establishes "required" and "permitted" PHI disclosures:
- ✓ Required disclosures under HIPAA must be made to:
  - to the patient and his/her personal representatives or third-party designees (with certain limited exceptions)
  - The Office for Civil Rights
- ✓ Permitted disclosures under HIPAA mean situations when a covered entity is permitted, but not required, to disclose PHI without first obtaining written authorization from the patient.
  - Examples of permitted disclosures include, with certain important exceptions:
    - as needed for treatment, payment or healthcare operations
    - as required by law
    - for judicial and administrative proceedings
    - for law enforcement purposes
    - for public health activities
    - for de-identified information
- ✓ While a patient generally has the right to access his or her own PHI, there are certain exceptions when PHI can be denied such as:
    - psychotherapy notes
    - information compiled in anticipation of, of for use in a civil, criminal or administrative action or proceeding
    - information provided by non-health care provider on promise of confidentiality if access would be reasonably likely to reveal the source of the information
    - PHI not maintained in a DRS

☐ Make sure you have the proper safeguards in place and have conducted the necessary staff training.
- ✓ Covered entities must take certain steps to safeguard PHI, such as:
  - maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI
  - train all workers on the policies and procedures relating to PHI as necessary and as appropriate so each member of the workforce can fulfill his/her job functions
  - implement policies and procedures relating to PHI that comply with the relevant standards, implementation specifications, and other requirements.
    - policies and procedures must be reasonably designed and may take into account the size of and the type of activities that relate to the PHI maintained by the covered entity

- ☐ Keep in mind that:
  - ✓ covered entities must obtain the individual's written authorization for any use or disclosure of PHI that is not otherwise permitted or required by the Privacy Rule
  - ✓ individuals have the right to receive a Notice of Privacy Practices that contains certain required information, such as information regarding:
    - how a CE may use and/or disclosure his/her PHI
    - some of a CE's legal duties with respect to protected health information
    - patient rights under HIPAA
    - Model Notices of Privacy Practices are available through the Department of Health and Human Services (HHS)
      - o A sample Notice of Privacy Practices is also available in the *ADA Complete HIPAA Compliance Kit*

- ✓ While the federal regulation allows providers 30 days (with one 30-day extension) to act on any request for access to PHI, HIPAA does not preempt more stringent state law so be sure check state requirements.
- ✓ When a patient asks for a copy of his or her PHI, the PHI should be:
  - provided in the form and format requested if it is readily producible
    - o whether a specific format is readily producible depends on the CE's capabilities, not its willingness to do so
      - for instance, a scanned PDF version of PHI may be readily producible but a CE would not be required to buy a scanner for this purpose.
      - Similarly, a Microsoft Word version of paper PHI may not be readily producible.

- ✓ Covered entities:
  - may require that all requests for access to PHI be in writing
    - o may require and provide a specific form for this purpose
      - o a sample form, the Sample Request for Access, is included courtesy of the *ADA Complete HIPAA Compliance Kit*
    - o must inform individuals of any requirements for requesting PHI
      - cannot create barriers to requesting or releasing PHI
      - cannot unreasonably delay access
      - should take reasonable steps to verify the identity of the individual requesting the PHI
        - o can require oral or written verification or authentication controls if the request is submitted electronically
      - that deny access to PHI:
        - o must follow specific rules and may require assistance of legal counsel. For example, a denial be in writing, contain specific information, and be sent within 30 days of the request for access
        - o must give individual access to any other PHI requested to the extent possible after excluding any denied PHI
        - o must follow specific procedures if the patient requests review of the denial
  - o must send the copy of PHI to another person designated by the individual if the individual so requests, as long as the request is in writing, signed by the individual, and clearly identifies the designated person and where to send the copy.

Individual requests for access to PHI differ from HIPAA authorizations in that:

- ✓ covered entities are required to provide an individual access to his or her own PHI, including sending PHI to the individual's designee;

- ✓ an individual does not need to sign a HIPAA authorization when requesting access to his or her own PHI
- ✓ a signed HIPAA authorization is required for a PHI disclosure not required or permitted by HIPAA
- ✓ there is a 30 day deadline for responding to requests for access to PHI (with one 30-day extension); there is no deadline for disclosure regarding HIPAA disclosures pursuant to a HIPAA authorization
- ✓ fee limits apply to requests for access to PHI; however, HIPAA does not address fees for disclosures under HIPAA authorizations, although state law limits may apply

Make sure that you and your staff:

- ✓ have policies and procedures for compliance with the Privacy Rule, such as policies and procedures for responding to patients' requests for access to their PHI
- ✓ reasonably safeguard PHI to limit "incidental disclosures;" for example:
  - o refrain from having discussions that might involve PHI in public areas, such as open bays and administrative areas since private information could be overheard by others
  - o follow common sense practices, such as speaking in low voices, having discussions behind closed doors whenever possible, using white noise or low music, to keep discussions private
  - o hold any conversation that discusses patients' health and/or financial information to a more private area, preferably one with a door
- be aware of patients' body language and, if someone looks uncomfortable, move the discussion to a location that offers more privacy
- be aware of situations when minor patients reach the age of majority since this transition may impact your ability to discuss PHI with parents and guardians, even if the parents or guardians accept responsibility for paying for treatment
- consider asking patients to provide a list of individuals who can be present for discussions that may involve PHI
  - o make sure the name(s) of those individual(s) are detailed in the patient's record as being identified by the patient as someone who can be in attendance for discussions that may involve PHI
  - o it's reasonable to infer that a patient has given implied consent for someone, such as a translator or caregiver, to be present for a discussion that may include PHI if they've invited or allowed that person to be present

- ✓ When a patient requests a copy of his or her PHI, providers may charge a reasonable, cost-based fee to provide a paper or electronic copy of the requested PHI. That fee must be limited to:
  - the cost of labor for time spent on making copies
    - o the cost of labor for time needed to search for and retrieve the PHI cannot be charged
  - the cost of supplies for creating a paper copy, or electronic media if the patient requests that the electronic copy be provided on portable media, such as a CD, USB drive, or similar portable media/device
  - the cost of postage if the patient requested the PHI be mailed
  - those who do not want to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically may charge a flat fee, not to exceed $6.50.
    - o More information about HIPAA access right fees that can be charged to individuals for copies of their PHI is available in the U.S. Department of Health and Human Services' FAQ on Individuals' Right under HIPAA to Access their Health Information 45 CFR §

164.524. Specific details are available in the answer to the question "How can covered entities calculate the limited fee that can be charged to individuals to provide them with a copy of their PHI?"

- Other resources available through HHS include A Health Care Provider's Guide to the HIPAA Privacy Rule: Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care.

Resources:

HHS Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524
HHS Model Notices of Privacy Practices
ADA's Sample Request for Access, from the *ADA Complete HIPAA Compliance Kit*
HHS FAQ on Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524
HHS A Health Care Provider's Guide to the HIPAA Privacy Rule: Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care