Managing the Regulatory Environment

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

ADA Tip Sheet on the HIPAA Security Rule

Different safeguards are required by the HIPAA Security Rule to protect patients' electronic protected health information (e-PHI). This tip sheet provides general information about certain aspects of the Security Rule. Additional information is available from the Department of Health and Human Services' (HHS), such as Security Rule, HIPAA for Professionals, and Security Rule Guidance Material. The website also includes information on other OCR rules that relate to dentistry; the page titled Privacy Rule: General Topics may be of particular interest.

Compliance with the requirements of the Security Rule involves many steps regarding the different types of safeguards including those detailed below. It is more encompassing than simply the electronic submission of claim forms and includes safeguarding physical and technological assets as well as having the appropriate administrative, physical, and technical safeguards are in place to protect patients' information and to ensure the practice's compliance with the Security Rule.

- ☐ Administrative safeguards include safeguards such as:
  - ✓ conducting a risk analysis and implementing risk management protocols
  - ✓ having written policies and procedures
  - ✓ documenting workforce training
  - ✓ designating someone on staff to serve as the practice's security official
  - ✓ periodically updating the risk analysis
  - ✓ identify and respond to suspected or known security incidents and mitigate harmful effects, document security incidents and their outcome
  - ✓ documenting sanctions applied if security policies and procedures aren't followed
  - ✓ Having a compliant business associate agreement in place with each business associate
  - ✓ implementing – and following – appropriate steps to terminate access to e-PHI when access is no longer appropriate, such as when employment is terminated
  - ✓ managing passwords

- ☐ Physical safeguards are the mechanisms that protect electronic systems, buildings, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion. They include safeguards such as restricting physical access to e-PHI and retaining computer backups. Physical safeguards include safeguards such as:
  - ✓ Limiting facility access by:
    - implementing contingency operations to allow facility access to support restoration of lost data in the event of an emergency
    - making sure authorized personnel can access any e-PHI that's stored in a separate, secure location, such as somewhere away from the office or in the cloud, during emergencies
    - ensuring that any offsite storage is secure and maintaining a business associate agreement
  - ✓ having a facility security plan; the plan may, as appropriate, addresses the use of features such as:
    - keys

- alarms
- locks
- key codes
- building security features, such as limiting access to appropriate personnel

✓ implementing access control and validation procedures such as visitor control and control of access to software programs for testing and revision:

✓ implementing sufficient workstation security practices to protect equipment used by doctors and staff while working in the practice and when working remotely

- ensuring that the physical environment of the workstation sufficiently protects any data that might be visible on screens

✓ establishing device and media controls, such as safeguards to ensure the secure storage of data and the secure transportation and disposal of data any devices used to store it

☐ Technical safeguards include safeguards used to protect data and to control access to it. Examples include:

✓ using access control and validation process to restrict ability to access PHI

✓ using authentication controls to verify that the person signing onto a computer is who he or she claims to be

✓ encrypting and decrypting data during electronic storage(e.g., on a hard drive) and/or transmittal (e.g., via email or e-fax, text, and in-office communications)

✓ implementing electronic automatic logoff procedures that terminate an electronic session after for a certain period of time

✓ implementing audit controls to examine activity in information systems, such as audit trail records to help detect inappropriate access to e-PHI

✓ having process in place that prevent the willful and/or accidental alteration or destruction of e-PHI

☐ Keep in mind that:

✓ An unauthorized disclosure of PHI, even if it occurs accidentally, may an impermissible disclosure that violates federal law.

✓ it's a good business practice for all covered entities and business associates that maintain e-PHI to encrypt that information, and HIPAA requires encryption wherever reasonable and appropriate to protect PHI

- Appropriate encryption of electronic PHI is a "safe harbor" in the event that a data breach occurs

☐ Take steps to help prevent breaches, such as:

✓ always verifying that any person or entity seeking access to PHI has permission to access it

✓ evaluating the risk to e-PHI when stored on removable media, mobile devices and computer hard drives

✓ encrypting data at rest, such as data on any desktop or portable device or media used to store e-PHI, and data in transit, such as data being sent via email

✓ taking reasonable and appropriate measures to safeguard e-PHI, which may include:

- store all e-PHI to a secure network so it's properly backed-up
- encrypt any data stored on portable/movable devices and media
- use a remote device wipe to remove data when a device is lost or stolen
- use appropriate data backup

- train staff members on ways to effectively safeguard data and the importance of promptly reporting any security incident or breach
- document all administrative, physical and technical safeguards in place and ensure that staff is aware of them

✓ reminding staff to physically safeguard areas where paper records are stored or used
- paper documents should be kept confidential and secured in locked cabinets
- be aware that every state has its own requirements regarding dental record retention schedules
- no PHI, including stickers, should ever appear on the front of any chart
- never leave any chart unattended
- limit the PHI that's on any printed schedule
- patient sign-in sheet may be used as long as the information is strictly limited (e.g., don't include the purpose of the visit)
- recall and/or appointment reminders are permitted by HIPAA as long as the information is strictly limited (e.g., the reminder may contain the patient's name, date, time and location of the dental practice, but not the purpose of the visit or any pre-operative or post-operative instructions)
- paper documents such as patient charts, treatment plans and payment receipts, should be properly destroyed in accordance with applicable law; e.g.:
  - shred documents and file any documentation that confirms that paper records were destroyed appropriately

☐ And, although the points below relate to HIPAA Privacy rulings and not the Security Rule, it's important to 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:
  - 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
  - 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
  - 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
  - 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
  - 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

Resources: HHS Security Rule
HHS HIPAA for Professionals
HHS Security Rule Guidance Material
HHS Privacy Rule: General Topics