HIPAA Safeguards

Dentists and their staffs hear prescriptive information about safeguarding patient information, for example, “paper records must be kept in locking file cabinets” and “sign-in sheets cannot be used.” Prescriptive information is clearly stated and easy to understand, but is it all really required by HIPAA? Following is 45 CFR §164.530(c) on safeguards required by HIPAA. It is applicable to all forms of protected health information (PHI) — hard copy, oral, and electronic.

1. **Standard: safeguards.** A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

2. **Implementation specification: safeguards.**
   
   i. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.
   
   ii. A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

As you can see, there is little detail on how to comply. The HIPAA Privacy Rule does not prescribe any specific practices or actions (generally referred to as “safeguards”). However, the HIPAA Security Rule, which became effective a few years after the Privacy Rule did, does require specific safeguards. Both rules allow a covered entity to take a flexible approach when considering how to protect patient information. A covered entity needs to consider its particular circumstances, such as impact on patient care, the size of its organization, and the financial and administrative burden of implementing a specific safeguard. A covered entity is not expected to absolutely protect patient health information from all threats and risks, but is expected to implement reasonable safeguards.

Following is an example of a deliberative process to determine what may be reasonable safeguards for paper chart storage in a dental practice. Dr. Gray is a solo practitioner with one front desk staff and one dental assistant. Her practice has been located for the past 15 years in a strip mall. Charts are stored in non-locking file cabinets located behind the front desk/counter. There is not a lot of extra space in the practice or in the front desk/counter area. The front desk/counter is situated behind a wall with a window and a door to the waiting room. The window is opened when patients check in or when staff communicates with individuals in the waiting room. The door is closed but unlocked during business hours. The area where charts are stored is observed by the dentist or staff during business hours. Both the front door and the door leading to the treatment area are locked when the practice is closed. Does Dr. Gray need to buy locking file cabinets for the charts?

Before answering the question, consider the following:

- What are the risks of not using locking file cabinets and what level of risk is it—low, medium, or high?
- Will changing the file cabinets cause minor or major disruption to the practice?
- Is the improved security benefit worth the total cost of the cabinets, (installation plus lost production time)?
Also consider how the analysis changes if Dr. Gray is planning to expand her practice and take over the space next to hers, if the strip mall provides after-hours security, or if there is a history of break-ins in the neighborhood. What if one staff member is absent and the front desk/counter is left unattended for a period – what should Dr. Gray do?

The covered entity must assess risk then determine reasonable and appropriate safeguards to implement. Consider another situation—the transportation of non-electronic patient information from one office to another. A covered entity must identify risks (theft and accident in this instance) and determine reasonable and appropriate policies and procedures for safeguarding the information.

**Safeguards to consider include:**

- Transporting the minimum necessary information
- Placing information in a case or bag, locking or non-locking
- Placing case or bag of information out of a passerby’s view of the vehicle’s interior
- No stops between offices

Yet another situation to consider is the fax machine and opportunities for impermissible disclosures. To minimize the risk of an impermissible disclosure, a covered entity may consider the following safeguards:

- Program often used fax numbers into the machine; verify fax numbers
- Double-check or confirm a patient’s fax number
- Use a cover sheet on fax transmissions containing PHI; cover sheet should include statement of confidentiality plus the contact name and telephone number of the dental practice privacy officer
- Time fax transmission so recipient can promptly pick it up
- Verify fax success
- Ensure received faxes are distributed to the appropriate person as soon as possible
- Ensure information on fax hard drive is erased prior to disposing the machine.

Remember, HIPAA regulations are intended to be flexible and scalable. A covered entity is not expected to absolutely protect patient health information from all threats and risks, but is expected to implement reasonable safeguards.

When a covered entity decides not to implement a privacy safeguard or an addressable security safeguard that offers the best protection, the covered entity should document the rationale for the decision. Determining what safeguards to implement can be a multi-factorial process. HIPAA does not require every dental practice to implement the exact same safeguards adopted by every other dental practice. Some privacy safeguards, such as keeping voices low when speaking about patient health information in places where the information can be overheard, can be universally implemented. Other safeguards, especially the addressable safeguards in the HIPAA Security Rule, can be assessed before determining whether to implement them.

The HIPAA Security Rule has 19 required safeguards and 16 addressable safeguards. Addressable safeguards should be implemented if a covered entity, after it conducts its risk analysis, deems the safeguard reasonable, appropriate and applicable.
The addressable safeguards include:

- implementing procedures for the authorization and/or supervision of staff members who work with patient information or in locations where it might be accessed;
- implementing procedures to determine that the access of a staff member to patient information is appropriate;
- implementing procedures for terminating access to patient information when employment of a staff member ends;
- implementing security reminders;
- implementing procedures to guard against and detect malicious software
- implementing procedures for periodic testing and revision of contingency plans; and
- implementing procedures for creating, changing, and safeguarding passwords.
- establishing procedures that allow access to the physical space where data is stored in support of restoration of lost data under a disaster recovery plan and emergency mode operations plan;
- implementing policies and procedures to safeguard the physical facility and equipment from unauthorized physical access and theft;
- implementing procedures to verify a person’s authorization to access facilities and software programs for testing and revision;
- implementing policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, walls, doors, and locks);
- creating a retrievable, exact copy of patient information before equipment is moved from where it is stored;
- automatic logoff (electronic procedures that terminate a session after a predetermined time of inactivity);
- implementing a mechanism to encrypt patient information whenever appropriate;
- implementing policies and procedures to prevent improper alteration of information on the system; and
- implementing mechanism to verify that patient information has not been altered or destroyed in an unauthorized manner.

The safeguarding of electronic PHI, however, does have specific requirements which can be found in 45 CFR §§ 164.306, 164.308, 164.310, and 164.312. The required Security Rule safeguards are:

**Administrative**

- conducting thorough initial and periodic analyses to determine potential risks to the security of patient information that is stored and used electronically;
- implementing practices to reduce identified risks and vulnerabilities;
- instituting a system to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- responding to security incidents;
- training staff (including unpaid volunteers and students who work in the practice) to be aware of and follow office information security policies and procedures;
- implementing a policy to sanction staff members who violate office information security policies and procedures; designating one staff person to be the Security Officer (similar to the designation of a Privacy Officer as required by the HIPAA Privacy Rule);
- establishing appropriate access levels for staff to patient records (determined by job requirements);
- assigning a unique name and/or number for identifying and tracking identity of information system users;
- establishing data backup and disaster recovery plans;
• establishing contingency plan to enable continuation of critical business processes for protection of the security of patient information while operating in emergency mode; and
• having business associate agreements that require compliance with Security Rule and notification of data breaches that occur with the respective business associate.

**Physical**

• implementing policies and procedures to limit physical access to a practice’s information system to authorized individuals for specified activities;
• implementing policies and procedures for workstation use that specify the functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings (includes tablets and PDAs);
• implementing policies and procedures to ensure the physical safeguard and security of workstations; and
• implementing policies and procedures governing receipt, security, transport, removal, re-use, and disposal of hardware and electronic media containing electronically stored protected health information.

**Technical**

• access controls, including unique user identification and emergency access procedure;
• audit controls (ability to monitor/track activity on the a practice’s information system); and
• person or entity authentication.