RECORD Storage HIPAA

https://hipaa.yale.edu/security/policy-guidelines-physical-security

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

1. **Medical records** and PHI **stored** in hallways that are accessible by unauthorized individuals **should** be in locked cabinets.
2. No open shelves in a **patient** or research subject area.
3. No open shelves in a hallway that allows access to individuals not authorized to access those **medical records** and PHI.
4. Medical Records and PHI should be stored out of sight of unauthorized individuals, and should be locked in a cabinet, room or building when not supervised or in use.
5. Provide physical access control for offices/labs/classrooms through the following:
    1. Locked file cabinets, desks, closets or offices
    2. Mechanical Keys
    3. ID swipes
    4. Alarm keypad systems (mechanical or electronic)
    5. Change keypad access codes on a regular basis
6. Assign someone to manage and document access issues (keys, card swipe, keypad access):
7. Identify individual(s) with the authority to grant access to an area

BEST PRACTICE in “shared offices”.

- Practitioners should have their own locking filing cabinet or storage unit.
- The next step is how to secure the locking filing cabinet or storage unit?
- When possible place the locking filing cabinets or storage units in a closet that is also controlled by a locking device.
- The GOAL is to prevent someone from easy access to records.

PSYCHOTHERAPY NOTES:
Psychotherapy notes, which may include more detailed or sensitive client information, must be kept separately from the general record in order to be afforded heightened protection under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

For example, health insurers cannot obtain them without a completely voluntary patient authorization.

Maintenance and security

APA's record-keeping guidelines also recognize the importance of multidisciplinary collaboration in providing patient care. Accurate records facilitate adjunctive treatment, such as medication management, coordinated care for chronic illness or family therapy intervention. Should an unforeseen illness befall the Practitioners, an up-to-date record facilitates the successful transfer of care.

Records may also be requested by the client, or his or her attorney, for other uses, such as divorce or other legal proceedings, applications for disability or life insurance, or requirements for certain types of employment.

Practitioners need to have a security plan that provides adequate protection for either paper or electronic records from loss or damage, and ensures only appropriate access by trained professionals or others with a legitimate need to see them.

With expanding wireless and computer technologies, client data may be kept in various electronic formats, such as emails, text messages and online scheduling calendars. Practitioners should be particularly cautious when exchanging protected health information via fax, email, text messaging and electronic claims submission.

Many Practitioners store patients' electronic records on their office computers, laptops and tablets. However, Practitioners must be vigilant in preventing unauthorized access to the data and protecting the actual equipment from theft. Data breaches reported under the HIPAA Breach Notification RULE * are frequently the result of theft, particularly of laptops and other portable electronic devices (retrieved 9/30/11).

Practitioners should store backup media as carefully as they do their original electronic files.

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

10 common HIPAA violations and preventative measures to keep your practice in compliance

Check out this link:

https://www.beckershospitalreview.com/healthcare-information-technology/10-common-hipaa-violations-and-preventative-measures-to-keep-your-practice-in-compliance.html