PEACE OF MIND

EXPERTISE

CHOICE

THE MEDPRO GROUP DIFFERENCE

Guideline

Record Retention

MedPro Group
a Berkshire Hathaway company

medpro.com

Contents

Introduction 1

Objectives 1

Record Retention Policies and Procedures 1

Patient Health Records 2

- Federal Requirements 2
- State Requirements 3
- Risk Management and Professional Liability Guidance 4
- Other Record Retention Considerations 5
  - *The Legal Patient Record 5*
  - *Electronic Versus Paper Records 5*
  - *Provider Specialty 6*

Business and Personnel Records 6

Destruction of Records 6

- Paper Records 7
- Electronic Records 7
- Documentation 8

Transfer of Records 8

Conclusion 10

Resources 10

Endnotes 10

Introduction

Healthcare practices generate and maintain many different types of records, including patient health records and business records. These records help practices maintain critical information and deliver quality service and care. Because of records' vital role, practices need to properly maintain and manage them throughout their lifecycle — from creation to destruction.

Objectives

The objectives of this guideline are to:

- Identify essential elements of formal record retention policies and procedures
- Discuss the regulatory requirements and claims/risk management considerations used to determine appropriate record retention policies and procedures for patient health records
- Review additional considerations for record retention, such as defining the legal patient record, determining appropriate processes for paper and electronic records, and considering provider specialty
- Describe the process for destroying records
- Review requirements for transferring records

Record Retention Policies and Procedures

To protect records, healthcare practices should develop and implement formal record retention policies and procedures. Doing so will help establish a systematic and organized approach to record management. Further, formal policies and procedures may help defend against allegations that records were deliberately or maliciously destroyed.

At minimum, record retention policies and procedures should include:

- The length of time records will be maintained
- A list of records that will be maintained onsite and offsite
- A definition of what documents constitute a "legal" record
- The form/manner in which the records are maintained (i.e., paper, electronic, or a combination of both)

- A designated individual (role) who is responsible for policy oversight, record maintenance, and initiating the destruction of records
- The methods for destroying records while preserving privacy and confidentiality (e.g., shredding, incineration, physical destruction of hard drives, high-level overwriting of electronic information, etc.)
- Requirements for documenting the destruction of records
- Backups and redundancies and how they're addressed in the destruction process (for electronic health records [EHRs])

Patient Health Records

Patient health records are an important part of patient care. They provide essential patient information, historical details about the course of care, and a record of services provided. Further, thorough and accurate records may play a crucial role in defending a malpractice claim. When developing record retention policies, healthcare practices should consider federal and state laws, accreditation and professional organization requirements, and professional liability recommendations.

> "Thorough and accurate records may play a crucial role in defending a malpractice claim."

Federal Requirements

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires covered entities (CEs), such as healthcare practices billing Medicare, to retain required HIPAA-related documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.[1] Examples of HIPAA-related documentation include:

- Notices of privacy practices
- Authorizations for the disclosure of protected health information (PHI)
- Business associate agreements (BAAs) or contracts
- Risk assessments and risk analyses
- Disaster recovery and contingency plans

- Information security and privacy policies
- Employee sanction policies
- Incident and breach notification documentation
- Complaint and resolution documentation
- Physical security maintenance records
- Logs recording access to and updating of PHI
- Information technology security system reviews (including new procedures or technologies implemented)[2]

Further, the HIPAA Privacy Rule requires covered entities to apply appropriate administrative, technical, and physical safeguards to protect the privacy of health records and other forms of PHI for as long as they are maintained.[3]

The Centers for Medicare & Medicaid Services (CMS) requires healthcare providers and organizations submitting cost reports to retain patient records for Medicare beneficiaries for at least 5 years after the closure of cost reports. CMS requires Medicare managed care program providers to retain records for 10 years. Medicaid requirements vary by state.[4]

State Requirements

Some states have specific requirements for the retention of patient health records. Often, these requirements are accessible via providers' professional licensing boards. In states that offer no specific requirements, the American Health Information Management Association (AHIMA) recommends that healthcare organizations "keep health information for at least the period specified by the state's statute of limitations or for a sufficient length of time for compliance with laws and regulations."[5]

Additionally, in some circumstances, the statute of limitations may not begin until patients realize that they have a basis for a claim. Thus, many practices automatically retain records for as long as practical based on patient volume and storage availability.

Many states also have specific requirements for the retention of diagnostic study results. In the absence of state guidance, healthcare practices should retain diagnostic study results for a minimum of 7–10 years. Diagnostic study results include, but are not limited to, X-rays and other imaging records, raw psychological testing data, fetal monitoring tracings, and data from electroencephalograms, electrocardiograms, and laboratory studies.

> "In some circumstances, the statute of limitations may not begin until patients realize that they have a basis for a claim."

Risk Management and Professional Liability Guidance

Coded data from MedPro Group's claims and suits opened between 2012 and 2021 indicate that 82 percent are opened within 3 years of the date of service, 96 percent are opened within 5 years of the date of service, and 99 percent are opened within 10 years of the date of service.

These malpractice claims statistics serve as the basis for the following risk management guidance, which should be used as a guide — not a rule — to determine length of record retention (after considering federal and state requirements):

- **Competent adults:** Maintain records at least 7–10 years after the last date of service. This usually allows sufficient time for the statute of limitations and extensions and other delays to be exhausted.
- **Incompetent adults:** Maintain records (a) until/unless the patient becomes competent (then follow guidance for competent adults), (b) at least 7 years after death, or (c) as long as possible (indefinitely).

Records Associated With Potential or Active Litigation

All records associated with incidents that could lead to litigation and all records that have been requested by an attorney or administrative agency (such as a licensing board) should be excluded from the practice's general retention policy and retained indefinitely.

These records should not be destroyed until the matter is fully resolved and only with the advice of the practice's professional liability carrier or attorney. If these records are not retained appropriately, a plaintiff's attorney may allege spoliation (i.e., that the provider destroyed evidence that they had a duty to retain).

- **Minors:** Maintain records at least through the state-specific statute of limitations after the child reaches the age of majority (18 years of age in most states). If the patient is 16 or 17 when last seen, it is prudent to retain the records for 7–10 years from that date.
- **Deceased patients:** States may have specific guidance for the retention of records for deceased patients. In the absence of state guidance, practices should consider retaining a deceased patient's records for 7–10 years from the date of the patient's death.

AHIMA recommends that health organizations (a) keep adult patient records 10 years beyond the most recent encounter, and (b) keep pediatric records up to the age of majority, plus the statute of limitations. AHIMA also advises organizations to permanently keep master patient/person indexes, birth and death registries, and registries of surgical procedures.[6]

Other Record Retention Considerations

The Legal Patient Record

Healthcare practices should develop policy statements that specifically define what each practice considers a "legal patient record." These policies should consider documentation that occurs during patient encounters as well as other types of communications, such as emails, patient portal interactions, text messages, etc. Defining the legal patient record will help providers and staff comply with documentation and retention standards.

Electronic Versus Paper Records

Although retention requirements do not differ based on record format (i.e., paper versus electronic), other aspects of retention — such as storage — may differ. Many healthcare practices have transitioned from paper to electronic records; as such, they might maintain both types of records.

> "Practices should develop processes to ensure careful quality control of all records that are scanned. Missing or illegible information in scanned records can jeopardize the quality of patient care and increase liability exposure."

An important consideration for healthcare practices is maintenance of paper records following implementation of EHR systems. State regulations might provide guidance on paper record retention requirements, and practices should be aware of specific guidance within their states. Further, practices should develop processes to ensure careful quality control of all

records that are scanned. Missing or illegible information in scanned records can jeopardize the quality of patient care and increase liability exposure.

Provider Specialty

Providers' specialties — or the nature of the procedures they perform — may influence record retention policies. For example, a provider who performs procedures using prostheses or implanted devices might find it prudent to retain records for an extended length of time. Conversely, a practitioner who performs less complicated procedures or therapies might find that a shorter retention period is reasonable.

Regardless of the circumstances, providers should ensure that, at minimum, their policies comply with federal and state laws and professional guidance.

Business and Personnel Records

In addition to patient health records, healthcare practices also generate various business-related records, such as contracts, billing documents, tax documents, organizational policies and procedures, etc.

Appropriately maintaining and managing these records is essential to reducing organizational risk. The practice's accounting firm or the Internal Revenue Service (IRS) may offer useful information about the retention of business records.

Federal and state government guidelines may specify record retention requirements for employee files and other personnel information. For questions or advice related to the maintenance of personnel records, healthcare practices should contact their attorneys or management consultants.

Additional resources are listed in the "Resources" section of this guideline.

Destruction of Records

Destruction of records, when they are no longer needed, is an important component of the document lifecycle. As such, healthcare practices should (a) include details about record destruction in their record retention policies, and (b) implement procedures to ensure a consistent approach to destruction.

Maintaining confidentiality of PHI is paramount during the destruction of records. HIPAA requires CEs to "implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information."[7]

"Maintaining confidentiality of PHI is paramount during the destruction of records."

Some states also have specific requirements relative to the destruction of records. When developing retention and destruction policies, practices should follow both federal and state requirements. AHIMA also offers detailed information about the retention and destruction of health information.

Paper Records

When paper records are identified for destruction, they should be shredded, incinerated, etc. — preferably by a company that provides such services. The method of destruction should ensure that the records are unreadable and unrecoverable.

The company contracted to destroy the records should provide the service at the healthcare facility so the destruction can be confirmed. If the company will destroy records that contain PHI, the practice will need to have a HIPAA BAA with the vendor. Visit the U.S. Department of Health and Human Services website to learn more about HIPAA BAAs, and use MedPro's *Checklist: Due Diligence of Business Associates* to assess your screening process for business associates.

Electronic Records

As technology has advanced over the years, most healthcare practices have transitioned to electronic records. Electronic records, like paper records, must be "destroyed with a method that provides for no possibility of reconstruction of information."[8] To this end, the HIPAA Security Rule requires CEs to implement policies and procedures for:

- Addressing the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored
- Removing electronic PHI from electronic media before the media are made available for reuse[9]

Depending on the approach, destruction of electronic records may involve overwriting of electronic media, magnetic degaussing, pulverizing, incinerating, cutting, etc. Practices should select the approach that is appropriate for the type of data being destroyed.

Further, before selling or destroying computers or any media that holds information, a competent employee or service provider should destroy all electronic documents and database records stored on the equipment.

Documentation

As part of the record disposal process, healthcare practices should establish a method to document the destruction of records. AHIMA recommends that organizations maintain a destruction log that includes:

- Date of destruction
- Method of destruction
- Description of the disposed records (e.g., name, date of birth, social security number, unique patient identifier, etc.)
- Inclusive dates
- A statement that the records were destroyed in the normal course of business
- The signatures of the individuals supervising and witnessing the destruction[10]

AHIMA offers a Sample Certificate of Destruction for healthcare organizations to use as a documentation template.

Transfer of Records

If a healthcare practice is closed or sold, arrangements must be made for retention of original records for the appropriate amount of time. Under no circumstances should original records be given to patients.

In some instances, healthcare providers who are selling or closing practices may choose to store their records themselves. Many providers retiring today do not have their records in electronic formats. When this is the case, the doctor assumes responsibility for storing the paper records.

In addition to the space requirements, this approach can be problematic if the records have not been maintained in an ordered system and former patients request copies of their records (to which they are entitled under HIPAA).

Patient Record Requests

Under HIPAA, healthcare providers' responsibility to provide patients with copies of their records does not terminate when providers retire or leave their practices. As long as providers still possess the records, they must provide copies if patients request them.

A second document maintenance option is the contracted services of a records storage company. Although these companies' fees might be substantial, they offer several advantages. First, they will pick up the records and store them in a climate-controlled facility, which can protect them from environmental damage (e.g., dampness, mold, vermin, etc.). Second, these companies usually are bonded or insured, thereby reducing a provider's liability exposure if stored records are damaged, destroyed, or stolen while in the records storage company's possession.

Third, records storage services are able to respond to patients' requests for records. Patients can be referred directly to the storage service, which then will locate and copy the records and collect the fee from the patient. (HIPAA allows a reasonable fee to be charged for locating and copying records.)

At the time of records transfer, a records storage company will execute a BAA with the storing practitioner. This HIPAA-required document obliges the storage company to protect the confidentiality of PHI contained in the patient records to the same standard that the healthcare provider must protect it. Through the BAA, the provider and the patients are assured that the PHI will be secure.

Another possible option for a provider who is selling a practice is for the purchasing practitioner to become the custodian of the selling practitioner's records through execution of a BAA. In this case, in addition to compliance with HIPAA Privacy and Security Rules, the BAA should specify that the custodian will provide the selling practitioner with access to the physical records upon reasonable notice (such as 2 business days), and that the custodian will not release or dispose of any original records without the seller's written authorization.

Patients who continue their relationship with the practice can authorize release of their records to the purchasing physician (who is already in physical possession of the records) as part of new patient consent processes. Records for patients who leave the practice can ultimately be placed in storage or archived.

Regardless of how practitioners choose to store their records, compliance with HIPAA remains essential.

Conclusion

Healthcare practices are responsible for various types of records, including patient health records, business records, personnel records, and more. To ensure consistency and accountability, practices should implement policies and procedures for the retention, maintenance, and destruction of records.

These policies should be based on federal and state requirements, general risk management and professional guidance, and advice from the practice's attorneys, management consultants, accountants, and other sources of expertise/authority.

Resources

- American Academy of Pediatrics: Medical Record Retention
- American Health Information Management Association: Retention and Destruction of Health Information
- HIPAA Journal: Record Retention Requirements
- MedPro Group: Guideline: Closing a Healthcare Practice: Guideline Strategies and Risk Management Considerations
- National Institute of Standards and Technology: Guidelines for Medical Sanitation

Endnotes

[1] Centers for Medicare & Medicaid Services. (2012, August 21). Medical record retention and media format for medical records. *MLN Matters*, SE1022. Retrieved from www.cms.gov/files/document/mlnpodcastmedicalrecordretentionandmediaformatpdf

[2] Adler, S. (2023, April 9). HIPAA retention requirements. *HIPAA Journal.* Retrieved from www.hipaajournal.com/hipaa-retention-requirements/

[3] U.S. Department of Health and Human Services, Office for Civil Rights. (2009, February 18). *Does the HIPAA Privacy Rule require covered entities to keep patients' medical records for any period of time?* Retrieved from www.hhs.gov/hipaa/for-professionals/faq/580/does-hipaa-require-covered-entities-to-keep-medical-records-for-any-period/index.html

[4] Centers for Medicare & Medicaid Services, Medical record retention and media formats for medical records.

[5] American Health Information Management Association. (2013). Retention and destruction of health information. Retrieved from https://library.ahima.org/PB/RetentionDestruction#.XuoWeC5KhPY

[6] American Health Information Management Association. (2011). Appendix D: AHIMA's recommended retention standards. In *Retention and destruction of health information.* Retrieved from https://bok.ahima.org/doc?oid=105019

[7] U.S. Department of Health and Human Services, Office for Civil Rights. (2009, February 18). *What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?* Retrieved from www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html

[8] AHIMA, Retention and destruction of health information.

[9] HIPAA Privacy and Security Rule, 45 C.F.R. § 164.310(d)(2)(i).

[10] AHIMA, Retention and destruction of health information.

medpro.com