ATTN: ALL PROVIDERS

Medical Record Retention/Destruction

Medical Records (MR) retention is the practice of securely and confidentially storing patient charts. A variety of factors impact medical record retention regulations; they can vary depending on the type of record (medical practices and hospital) and/or based on whether an adult or a minor.

Lack of file space and volumes of information are just a couple of issues that create labor-intensive maintenance processes for retrieval of medical records. Before EMRs digitized patient charts, physicians often ran out of physical storage space and had to destroy certain records. However, even EMRs don't have unlimited storage and memory, so the need to destroy records hasn't entirely disappeared.

*Keep in mind that destruction practices in violation of medical records retention laws are grounds for lawsuits.*

Federal Regulations related to MR retention and destruction were updated in 2021. The updated guidelines give information on updated access requirements as well as advise how long to keep MR documentation.

Since state laws can be modified by the state legislature, check regularly to make sure that new legislation is not being considered on record retention and/or destruction.

MEDICAL RECORD RETENTION

The life cycle of medical records begins when information is created and ends when the information is destroyed. The duration for which providers must store records varies by state and additional federal guidelines also apply.

At a minimum, record retention policies must:

- Ensure patient health information is available to meet the needs of continued patient care, legal requirements, research, education, and other legitimate uses of the organization
- Include guidelines that specify what information is kept, the time period for which it is kept, and the storage medium on which it will be maintained (e.g., paper, microfilm, disk, tape)
- Include clear destruction policies and procedures that include appropriate methods of destruction for each medium on which information is maintained

There is no single standardized record retention schedule that organizations and providers must follow. Instead, a variety of retention requirements must be reviewed to create a compliant retention program.

*In the absence of direction from a STATE statute, follow federal regulations.*
Federal requirements:

- HIPAA: Medical records must be retained for a **minimum of 6 years**
- Hospitals:
  - Medical records must be retained in their original or legally reproduced form for a period of at least **5 years** after the date of discharge.
  - For minors, medical records must be retained for **3 years after the patient becomes of age** OR **5 years after the date of patient discharge**, whichever is longer
- CMS: CMS is the federally funded Medicare and Medicaid programs.
  - The CMS Hospital Conditions of Participation and Interpretive Guidelines require providers to maintain medical records for **7 years** from the Date of Service (DOS).

Louisiana requirements:

- Medical Providers: **6 years** from the date a patient is last treated
- Hospitals: **10 years** from the date a patient is discharged

There are a variety of unique medical records that have much lengthier requirements:

- Research records or studies that are related to cancer patients must be maintained for **30 years**, per the Federal Drug Administration (FDA).
- Health care providers who administer vaccines are required by the Center for Disease Control (CDC) to keep a **permanent medical record of vaccinations**. This requirement has become increasingly relevant with the large influx of COVID-19 vaccinations. Those who provide vaccinations are required to record the date of administration, vaccine manufacturer, address of clinic and other information that is tied to a recipient and must store this **permanently** in electronic or paper form.

A longer retention period may be prudent for organizations and providers, since the statute for malpractice lawsuits may not begin until the potential plaintiff learns of the causal relationship between an injury and the care received. Under the False Claims Act (31 USC 3729), claims may be brought up to **7 years** after the incident; however, on occasion, the time has been extended to **10 years**.

**MEDICAL RECORD ACCESS REQUIREMENTS**

HIPAA privacy regulations allow patients the right to collect and view their health information, including medical and bill records, on-demand. A request for information must be granted within 30 days of the request. If there are extenuating circumstances, the covered entity must provide a reason within that 30-day time frame, and the records must still be provided within 60 days.

CMS recognizes that providers may rely upon an employer or another entity to maintain MR. However, if a provider receives a MR request, the provider is responsible for providing the medical records to CMS or one of the Medicare contractors.

**MEDICAL RECORD DESTRUCTION**

Destruction of patient health information by an organization or provider must be carried out in accordance with federal and state law pursuant to a proper written retention schedule and destruction policy approved by appropriate organizational parties.

As with medical record retention, there is no single standard destruction requirement. In the absence of any state law to the contrary, organizations must ensure paper and electronic records are destroyed with a method that provides for no possibility of reconstruction of information. Records involved in any open investigation, audit, or litigation must not be destroyed until the litigation case has been closed.
Organizations must maintain documentation of the destruction of health records permanently and include the following:

- Date of destruction
- Method of destruction
- Description of the disposed records
- 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

The HIPAA Privacy and Security Rules do not require a particular disposal method, however covered entities must ensure that their workforce members receive training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member.

The HIPAA Privacy Rule (45 CFR 164.530(c)) requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. This means that covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. Under the HIPAA Privacy Rule, when destruction services are outsourced to a business associate the contract must provide that the business associate will establish the permitted and required uses and disclosures and include the following elements:

- The method of destruction or disposal
- The time that will elapse between acquisition and destruction or disposal
- Safeguards against breaches
- Indemnification for the organization or provide for loss due to unauthorized disclosure
- Require the business associate to maintain liability insurance in specified amounts at all times

The HIPAA Security Rule requires covered entities to implement safeguards to ensure the confidentiality, integrity, and availability of ePHI (i.e., PHI in electronic form). The HIPAA Security Rule (45 CFR 164.310(d)(2)(i) and (ii)) requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.

RESOURCES:

- MEDDATA News Blasts: [https://www.medtronsoftware.com/](https://www.medtronsoftware.com/)

MEDDATA News Blasts: [https://www.medtronsoftware.com/](https://www.medtronsoftware.com/)

For assistance or any questions, contact MDS/MSI: From MEDPM or MEDEH Sign On screens, double click on ‘helpdesk@medtronsoftware.com’ to compose an email which will automatically create a ticket in our ticketing system. The ticketing system will then send an automated reply with your ticket # for all future correspondence related to your question/concern.