Mishandling Medical Records: A Guide to Preventing Disaster

Shred Nations | @ShredNations

Table of Contents

Introduction

Medical records are mainstay of the healthcare industry. The information they contain details the health history of a patient, and is unfortunately also one of the most sought after sources of personal information for data thieves as well.

In an effort to better protect the privacy of patient medical records, state and federal laws like the Health Insurance Portability and Accountability Act (HIPAA) have been introduced in order to clearly define the proper methods for storing and destroying medical records once they have passed their retention period.

Despite this, numerous data breaches and steep fines for privacy violations have rocked the healthcare industry over the past decade, making it imperative that healthcare providers continue to emphasize the preservation of protected health information (PHI), both for their sake as well as their patients.

When it comes time for medical records to be destroyed after they are past their required period of retention, it's important that healthcare providers realize that disposal of medical records in a dumpster is a violation of HIPAA and cause for steep fines.

In order to safely destroy medical records, many providers have instead turned toward the adoption of secure medical record shredding services. Medical record shredding is a way for healthcare providers to ensure a secure chain of custody and compliance with HIPAA and other medical record destruction regulations.

With this in-depth white paper, we explore the world of medical records, breaking down what they are and their different types, as well as the implications of mishandling medical records and how healthcare providers can take steps to protect themselves and their medical records from data breaches and identity thieves.

What Is a Medical Record?

Often used interchangeably with other terms like medical chart or health record, a medical record refers to the systematic documentation of an individual's medical and healthcare history.

This record usually includes a number of notes and comments from healthcare professionals over time, detailing their observations and administration of pharmaceuticals and therapies, test results, x-rays, and other records.

Because a single medical record will only contain the healthcare information for a patient within a single healthcare provider's jurisdiction, an individual may have multiple medical records simultaneously—one from their general physician, one from a neurologist, and one from their dentist's office, for example.

Medical records contain sensitive protected health information (PHI) about a person's health and history, and as a result, the expectations for preservation of privacy have created many ethical and legal problems for both those who have fallen victim to identity theft due to compromised medical records as well as the healthcare providers who have mishandled their patients' medical records.

In light of this, processes for the proper management of medical records have become a critically important focus for healthcare. Recent data breaches have not only shaken the industry to its roots and left people worried about the protection of their medical records—new laws like HIPAA and FACTA have also imposed heavy fines for healthcare providers who have mishandled the medical records of their patients.

Types of Medical Records

Since a single medical record will only contain the health history as documented by a single healthcare provider, there a various types of medical records an individual may have. Here are a few of the most common healthcare providers that seek secure storage and shredding for medical records:

- Business Associates
- Covered Entities
- Family Medicine
- Emergency Medicine
- Internal Medicine
- Neurology
- OB/GYN
- Pediatrics

Traditionally, medical records have been compiled and managed by the healthcare providers themselves via hard-copy documents.

Today however, technology has also advanced to the point that electronic health records (EHRs)—which allow healthcare providers themselves to electronically enter and manage a patient's medical record—are now widely used by large-scale institutions like hospitals in order to keep up with the large numbers of patients they see.

Paper Medical Record Storage

Many healthcare providers still use hard-copy medical records to track the health histories of their patients.

It may be because providers haven't scanned and converted their paper medical records to electronic format, they are still a small enough practice to manage the paper record inventory, or they are simply not interested in adopting an EHR at this time.

Regardless of the reason a provider may have for still favoring a paper-based medical record storage system, one constant to managing hard-copy medical records involves how they are disposed.

If a healthcare provider were to keep every single medical record for their patients indefinitely, not only would they be facing an issue in terms of their storage space—there are also state and federal record retention laws which define how long a medical record must be kept before it is safely destroyed.

As a result, many healthcare providers who deal with hard-copy medical records create a record retention schedule for their medical records in order to remain compliant with state and federal laws like HIPAA.

According to HIPAA, which refers healthcare providers to following the record retention laws for their state, providers are also required to apply appropriate safeguards to protect the privacy of patient medical records and PHI for as long as the record is required to be retained by state law—including throughout the record's disposal.

Electronic Health Records (EHRs)

With advancing technologies allowing for electronic information to be more easily stored, managed, and shared, many healthcare providers have adopted the use of electronic health records in their everyday operations.

Electronic health records have become widely popular among many hospitals due to their advantages over paper medical records.

EHRs eliminate the need for providers to search for previous paper records and also reduce to chances for duplicate copies and inaccurate data replication, as there is only one editable health record with an EHR.

Although EHRs have been able to simplify the medical record management process in many ways and help to eliminate some of the waste from paper medical records, there are often major privacy concerns over records being stored on a centralized server.

Besides the fact that electronic health records that are shared or exchanged via an internet connection are subject to the same network security concerns as any other data transaction online—their storage method of keeping all records in a central location can also spell trouble in the event of a data breach.

If a breach were to occur, an individual with unauthorized access to one medical file would also have access to an entire database of patient medical records. It is because of this far-reaching access in an EHR that between 2005 and 2016, there were 1,274 data breaches in the healthcare industry that affected a whopping 45.4 million patient medical records—proving just how much single data breach can impact a system that stores all its medical records in a single, centralized location.

Similar to paper medical records, EHRs are also subject to the rules for access, storage, and transmittal of electronic medical records as defined by HIPAA. When this act was passed in 1996, it laid out stricter regulations for electronic medical records in an effort to better preserve patient privacy, however there are still concerns as to whether these standards are foolproof.

There are many ways for both paper and electronic medical records to be mishandled or misused—whether intentionally or by accident—which pose threats to patient privacy as well as the security of healthcare providers, making it critical that providers ensure medical records are properly managed throughout their lifespan and up to their ultimate disposal in order to prevent identity theft or fraud.

Why Identity Thieves Want Your Medical Records

Medical records are often prized by identity thieves because unlike an errant email address or envelope that would give a potential identity thief a small amount of an individual's personal information, medical records contain a swath of personal information.

If medical records fell into the wrong hands, they would give an identity thief everything they need to assume a person's identity and use their information against them.

The protected health information contained in a medical record is what identity thieves use to identify, locate, or contact a single person (like scam phone calls), which these thieves then use to gain access to resources like obtaining credit or other health benefits in the individual's name.

In one instance, a Colorado man was billed $44,000 for a surgery he never had when an ex-convict checked himself into a hospital using the victim's stolen social security number.

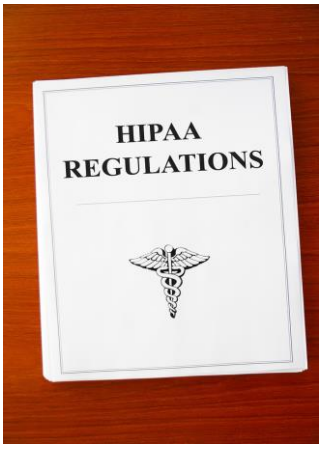
An individual's medical record contains a wide range of protected health information which can range from personal information like names and phone numbers to other financial information related to healthcare payments like social security numbers or health insurance accounts.

The following are the eighteen information types that are protected under HIPAA and formally defined as PHI:

- Account Numbers
- Biometric Identifiers (fingerprints, retinal scan, etc.)
- Certificate / License Numbers
- Device Identifiers and Serial Numbers
- Dates
- Email Addresses
- Fax Numbers
- Full Face Photos and Comparable Images
- Geographic Data
- Internet Protocol Addresses
- Health Plan Beneficiary Numbers
- Medical Record Numbers
- Names
- Social Security Numbers
- Telephone Numbers
- Vehicle Identifiers and Serial Numbers, Including License Plates
- Web URLs
- Unique Identifying Numbers, Characteristics, or Codes

It's not just with paper records that PHI comes into play—it's also important that healthcare providers using EHRs use proper encryption and other security measures to prevent their patients' medical records being compromised by a data breach.

How Employees Can Mishandle Medical Records



Maintaining the privacy of patient medical records is important not just for sake of the patient themselves—improper use or destruction of medical records can also impose heavy fines on healthcare providers.

HIPAA privacy and security regulations have cracked down on providers in recent years, and have little tolerance for any and all violations—whether it's accidental or not.

In some cases, medical record breaches have been caused by unintended disclosures like sending records to the wrong email, but there have also been cases where providers seemingly disregard HIPAA rules and simply toss old medical records in a dumpster.

Here are just a few instances of healthcare providers mishandling their patient's medical records:

- Four pathology groups and the former owners of a medical billing practice paid $140,000 to settle a HIPAA case after the billing information and medical records of 67,000 patients were improperly disposed of at a public dump.
- The Department of Health and Human Services and an Indiana community health provider called Parkview Health System reached an $800,000 HIPAA settlement in 2014. According to the investigation, Parkview employees had left unattended boxes containing the medical records of up to 8,000 patients on the driveway of a physician who they'd been told was not home that day.
- In 2015, the Department of Health and Human Services' Office for Civil Rights (OCR) settled with a Denver-based healthcare provider, Cornell Pharmacy, for $125,000 following the discovery of some 1,600 patient medical records left in an open container on Cornell Pharmacy's premises.

As you can see, HIPAA and other federal or state legislation governing the management of medical records doesn't leave much room for healthcare providers exposing their patients protected health information, making it imperative that providers ensure they take steps to properly protect records during their lifespan and throughout the destruction process.

Protecting Medical Records from Data Breaches and Identity Theft

Besides implementing measures to ensure your medical records are safely stored, a key aspect to managing medical records and keeping them out of the hands of identity thieves includes taking the proper steps to ensure their secure destruction as well.

As other instances of steep HIPAA fines in the past have demonstrated, proper destruction of medical records is not equivalent to leaving them in a dumpster.

According to the Department of Health and Human Services, a "properly destroyed" medical record is specifically defined as a medical record that has been "rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed."

In order to ensure medical records are being properly destroyed according the HHS standards, many hospitals and healthcare providers have adopted the use of secure shredding services to handle their destruction needs. Typically, there are two primary shredding options that providers use for properly destroying their medical records:

Mobile Shredding

With mobile shredding services, shredding box trucks equipped with industrial shredders conveniently come to the healthcare provider's curbside, shredding all medical records needing destruction while they watch. Because the documents are collected in locked bins and lifted into the shredder the same way a dump truck works, the shredding company will never come into contact with the sensitive medical records and PHI being shredded.

After the shredding is complete, the shredding company will provide a formal certificate of destruction, which guarantees that the service provided was compliant with all HIPAA and FACTA standards.

Offsite Shredding

Another popular option for proper medical record destruction, offsite shredding is ideal for healthcare providers like hospitals, which have a large volume of medical records they need regular destruction for. With offsite shredding, a shredding truck comes to your location and collects your documents before transporting them to a secure offsite shredding facility, making the service less-expensive since the truck doesn't need to stay on-site for shredding.

Due to the heavy emphasis on ensuring proper destruction for medical records, many healthcare providers worry about the chain of custody for medical records. However, similar to mobile shredding, healthcare providers are given certificates of destruction after the service is complete to guarantee the shredder's compliance with HIPAA and FACTA.

Conclusion

With rising numbers of data breaches and steep fines for HIPAA and other privacy violations, ensuring that protected health information is safely managed and destroyed has become a top priority for the healthcare industry.

An increasing number of practices and hospitals are taking steps to refocus their efforts on protecting the PHI of their patients, but nevertheless it is important that all healthcare providers ensure that all their medical record bases are covered by keeping a few last guidelines in mind:

- **Ensure Your Employees Are Informed and Up-to-Date –** Privacy laws and standards for managing and destroying medical records are constantly changing and being updated to keep up with the latest technology and privacy threats. Because so many data breaches and privacy violations in the medical industry are caused by employees mishandling records and not knowing what they did was wrong till it was too late, it's important your employees are aware.
- **Do You Have Proper Destruction Methods in Place? –** As past cases have demonstrated, improper disposal of medical records can result in steep HIPAA fines. Ensure that you have proper medical record disposal processes in place to ensure that you aren't exposing yourself or your patients to unnecessary risks.
- **Are Your Current Medical Records Being Stored Securely?** – If an employee leaves out medical records unsupervised or electronic health records are stored without proper encryption, a health provider runs the risk of violating privacy laws or having the electronic records hacked and stolen. As a result, it's important hospitals and health practices be sure to store medical records safely and securely—both for their sake as well as their patients.

Get Free, No-Obligation Quotes on Document Destruction Services for Your Medical Records

When it comes to the sensitive information contained in medical records and their high risk for being targeted by identity thieves, it's essential that healthcare providers continue to emphasize the proper management and storage of medical records throughout their retention schedule and up to destruction.

With a nationwide network of secure medical record shredding service providers, Shred Nations is able to help the healthcare industry prevent data breaches and safely protect their patients' PHI from identity theft. No matter whether you need destruction for paper medical records or EHRs, Shred Nations is your solution to all your document destruction needs.

To get started with scheduling a secure shredding or electronic media destruction service for your medical records, **just give us a call at (800) 747-3365, or simply fill out the form to your right to get free quotes on document destruction services in your area today!**

Additional Resources

Proper Protected Health Information (PHI) Disposal: With growing concerns over patient privacy and protecting medical records, more and more health practices and major hospitals are needing to up their standards for safeguarding patient Protected Health Information (PHI). Here, we take a closer look at PHI, breaking down the specifics like what it is, proper disposal methods, and the impact of foregoing the safe keeping of protected health information.

Protecting Your Company Against Fraud & Theft: The number of fraud, identity theft, and corporate espionage cases has drastically increased with new technological risks now adding to other external threats. With this in-depth white paper, we explore the often overlooked vulnerabilities in document management systems, providing detailed information on the steps a business can take to prevent falling victim to these threats themselves.

A Guide to Proper Data & Document Destruction: Although there several different ways a business can choose to store and manage their company documents, it is important that regardless of the method, your business take the steps to properly shred and dispose documents once they are no longer needed. In this in-depth white paper, we help to outline what media and information poses the greatest risk for being compromised and provide businesses the information they need to close those security gaps.

(*http://www.hhs.gov/hipaa/for-professionals/index.html*)

(*https://en.wikipedia.org/wiki/Medical_record*)