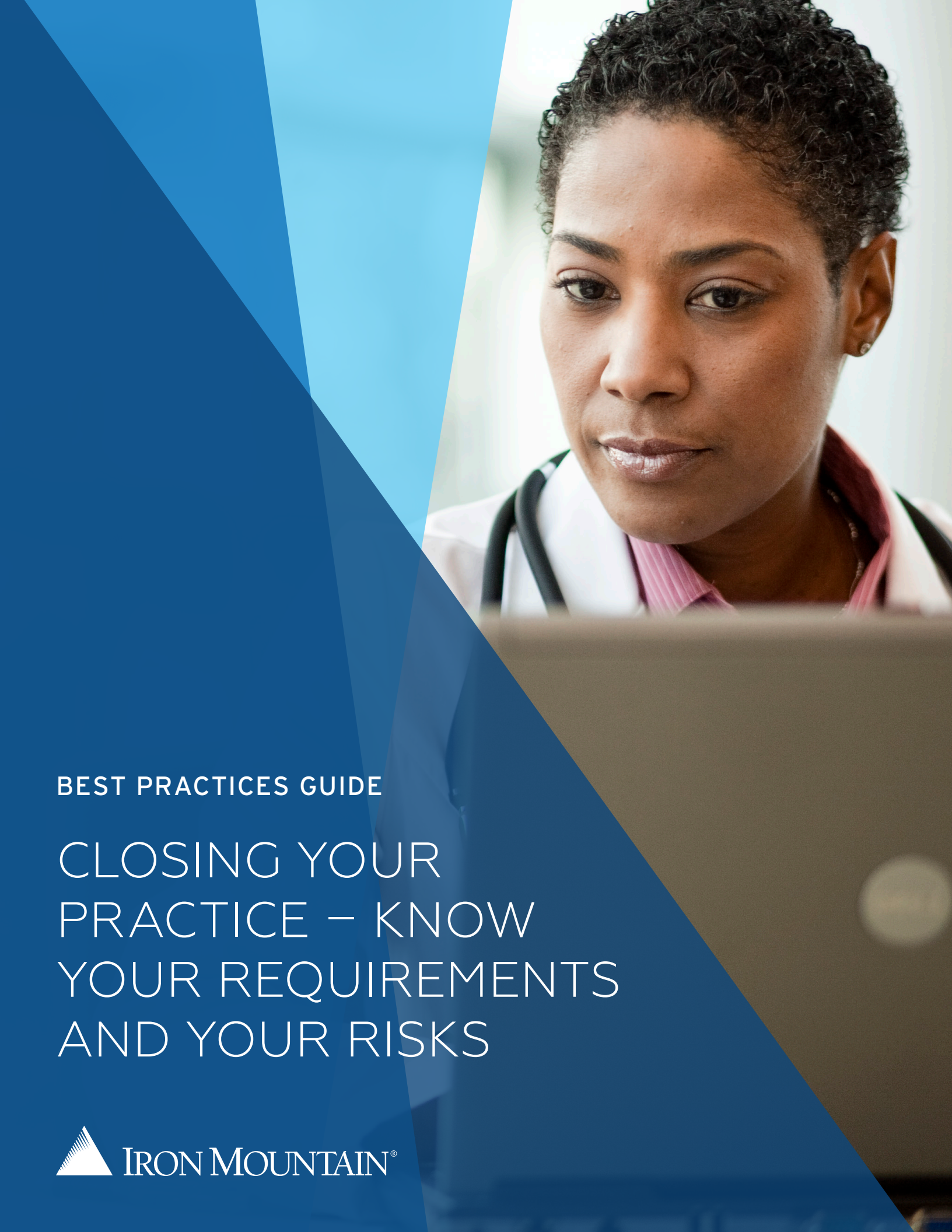


BEST PRACTICES GUIDE

CLOSING YOUR PRACTICE – KNOW YOUR REQUIREMENTS AND YOUR RISKS

IRON MOUNTAIN®

CONTENTS

INTRODUCTION

In the U.S., every state has requirements for closing a practice. Some states provide these as merely guidelines, while others have enacted these requirements into law, which could lead to fines and penalties if not followed correctly. When closing a practice, medical practices must interpret these laws and determine the steps required to ensure compliance and continuity of patient care. Prior to closing a medical practice, medical professionals should consult with a local attorney familiar with healthcare state laws, as well as a malpractice insurer to confirm the closure plan is compliant.

All states allow for a closed practice to transfer records to a third party, however it's important to ensure the records management provider understands and is able to comply with all the regulations associated with the storage and management of protected health information.

RECORDS MANAGEMENT BEST PRACTICES FOR CLOSING HEALTHCARE FACILITIES

DEPLOYING A RECORDS MANAGEMENT PROGRAM THAT ENABLES CONTINUITY OF CARE FOR YOUR PATIENTS AND PROTECTS YOU FROM THE LEGAL RISKS AND FINANCIAL PENALTIES ASSOCIATED WITH NON-COMPLIANCE

Closing a practice is never easy. Often you'll find long checklists of tasks you must complete in order to close, with little guidance in terms of the "how." Critical items such as records management must be addressed to ensure long-term compliance but often these complex processes are buried in the details of the broader closure plan. Any item overlooked or misinterpreted can leave you exposed to serious risks – both legal and financial.

To help you navigate this complex task, Iron Mountain's team of healthcare experts has assembled a list of best practices that addresses the elusive "how" of closing a medical practice compliantly. Follow these tips to protect yourself from legal risk and make sure your information remains secure and accessible throughout its retention.

- **Define and document retention based on federal, state and local laws for each record type.** This is a critical first step as it will lay the framework for the rest of your strategy. In order to identify a secure yet cost effective program for managing records throughout their retention, you must first define the criteria for assigning retention. You should consult with local legal resources with healthcare expertise and your malpractice insurance to verify compliance. For example, the type of record, date of the last visit and the age of the patient will need to be taken into consideration. Once you've identified key criteria, you will need to work with your records manager or partner to assign a retention period based on those criteria. This will not only aid in compliance but also serve as the foundation for how you will store and manage these records throughout their lifecycle.

- **Arrange for secure storage of medical records.** Providers are required to ensure patient records remain secure yet readily accessible regardless of whether or not your doors remain open. Given today's hybrid environment, this means providers must address both the physical and electronic records when preparing to close. The risks associated with storing records in a private residence or self-storage facility are often overlooked, and the location where the records are stored can also affect compliance in meeting required turnaround times for Release of Information. Physical records are often easily managed through a third party vendor, however - determining long-term storage for electronic records can be far more complex. To ensure the most cost-effective and secure management of these records, providers should take into consideration the number of records, the required retention and the anticipated activity against the records. In some cases, providers may choose to print and store a paper copy of the records from the EMR system to avoid the cost of supporting legacy technology or the increasing digital security risks. Records should be stored in a HIPAA compliant manner, and ensure timely response to requests for Release of Information.

- **Ensure that there is a process for the secure release of medical records to authorized users throughout their retention period.** The foundation of any records management program is to ensure the records are available to support continuing patient care. That means records cannot simply be hauled off to a self-storage warehouse or facility. They need to be stored and managed by a records management provider capable of providing that continued access. A qualified provider must understand legal and business requirements of the Release of Information. It's vital that they have the technology, staff and processes in place to enable authorized requestors to access the record as needed – and

be able to prove that PHI remains secure and that only the minimal information necessary is released. HIPAA requires an Accounting Of Disclosures to be maintained to track certain Release of Information activity, which can be cumbersome and lead to compliance violations if not followed correctly.

- **Tell patients how they can access their records going forward.** Patient notification regarding continued access of their medical records is a requirement for all closing practices. It's important to outline a clear process that details where the records are being stored, how the patient can request them and for what period of time they will remain available. Be sure to articulate the retention period assigned, making it clear that records will be destroyed and no longer available after expiration. Consult with an attorney familiar with the healthcare laws of your state to ensure your notification complies with all the requirements for closing a practice.

- **Make arrangements to destroy patient records upon retention expiration.** Once the retention period assigned to the patient records expires, it's important the records are securely destroyed. Moreover, it's important to employ a consistently implemented, defensible process that destroys all PHI beyond a recoverable state. Since the retention period is often many years after the practice closes, you want to make sure the plan for destruction happens automatically, and without additional intervention. Your plan for managing records for a closed practice should include pre-authorized destruction at the end of defined retention periods, with a Certificate of Destruction kept on file for compliance purposes.

- **Make arrangements to securely dispose of or destroy electronic systems and equipment housing sensitive PHI.** This is one step many providers forget. Often they make accommodations for the records but leave sensitive PHI vulnerable in day-to-day equipment such as copiers, fax machines, laptops or even cell phones. Just as critical to the compliance of your closing practices records management program is the wiping or secure destruction of any and all equipment that transmitted or housed protected healthcare information.

WATCHOUT! AVOID THESE SIX COMMON RECORDS MANAGEMENT PITFALLS FOR CLOSING PRACTICES.

1. **Insufficient retention:** Malpractice insurance may require longer retention to guarantee coverage or pending legal actions may require certain records to be held longer.

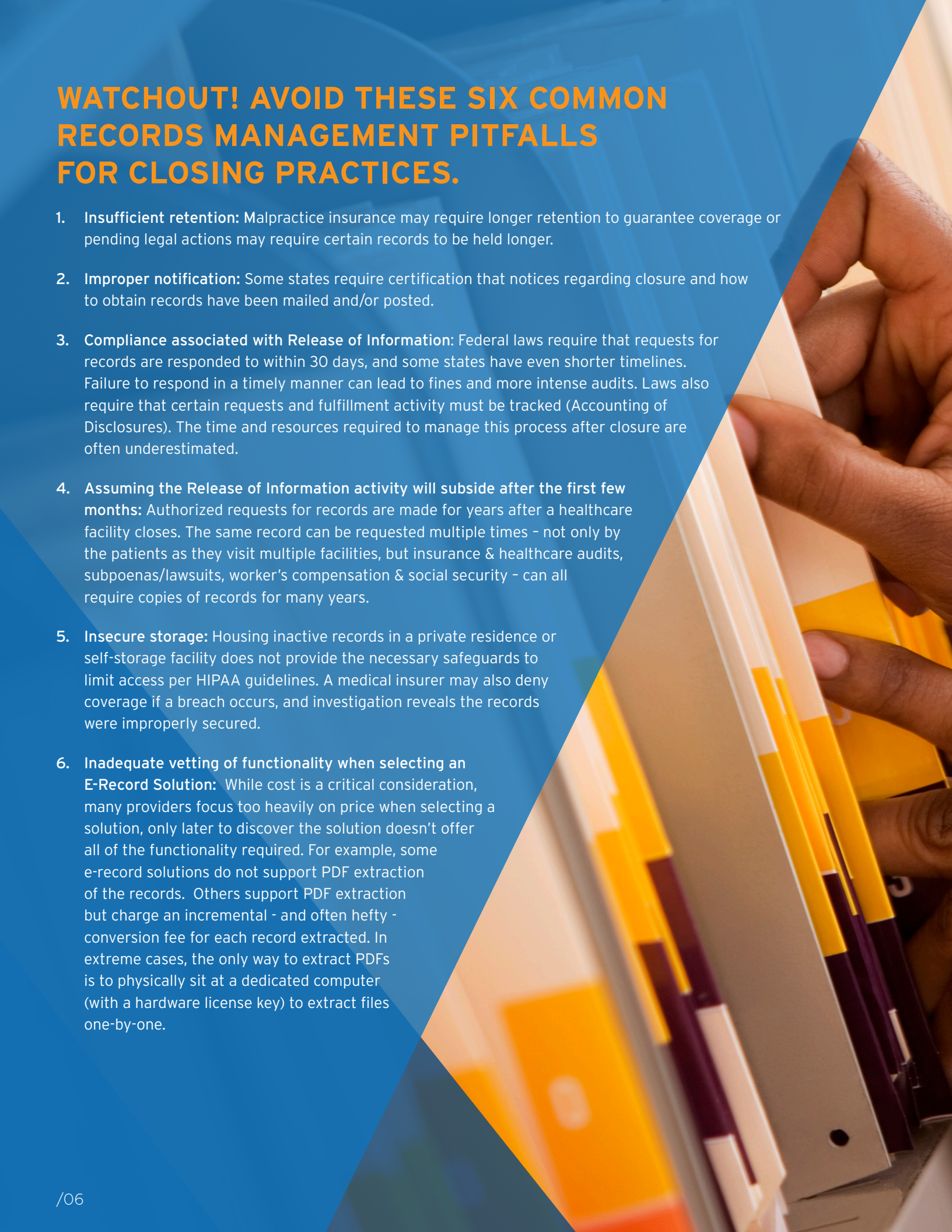
2. **Improper notification:** Some states require certification that notices regarding closure and how to obtain records have been mailed and/or posted.

3. **Compliance associated with Release of Information:** Federal laws require that requests for records are responded to within 30 days, and some states have even shorter timelines. Failure to respond in a timely manner can lead to fines and more intense audits. Laws also require that certain requests and fulfillment activity must be tracked (Accounting of Disclosures). The time and resources required to manage this process after closure are often underestimated.

4. **Assuming the Release of Information activity will subside after the first few months:** Authorized requests for records are made for years after a healthcare facility closes. The same record can be requested multiple times – not only by the patients as they visit multiple facilities, but insurance & healthcare audits, subpoenas/lawsuits, worker's compensation & social security – can all require copies of records for many years.

5. **Insecure storage:** Housing inactive records in a private residence or self-storage facility does not provide the necessary safeguards to limit access per HIPAA guidelines. A medical insurer may also deny coverage if a breach occurs, and investigation reveals the records were improperly secured.

6. **Inadequate vetting of functionality when selecting an E-Record Solution:** While cost is a critical consideration, many providers focus too heavily on price when selecting a solution, only later to discover the solution doesn't offer all of the functionality required. For example, some e-record solutions do not support PDF extraction of the records. Others support PDF extraction but charge an incremental - and often hefty - conversion fee for each record extracted. In extreme cases, the only way to extract PDFs is to physically sit at a dedicated computer (with a hardware license key) to extract files one-by-one.



BEST PRACTICE MODEL

So now that you understand the key requirements of properly managing records when closing a practice, the question becomes what is the best way to get there? Cobbling together a closure plan using multiple vendors and solutions introduces inconsistencies and unnecessary costs and risks. The safest and easiest means of deploying a cost effective and compliant program is to leverage a comprehensive solution that enables you to manage patient records throughout their entire lifecycle in a secure, proven and compliant manner.

There are several criteria you can assess to measure a vendor's ability to provide all of the services required to support a closing practice's records management program – and more importantly to ensure your health information management program is and remains HIPAA compliant.

- **Validate and Verify HIPAA Compliance.** Whatever solution you choose, it's important to verify HIPAA compliance. As you know, non-compliance is costly and you are not exempt of responsibility simply because you close your doors. To protect your reputation, patients and wallet–you'll want to ask questions about where and how the records will be stored. For example, are there safeguards to restrict physical access to the records? Can the release of records be tracked and managed to ensure that only the minimum information necessary is provided and only to authorized requestors? What controls and processes are in place to protect PHI at rest, in transit or upon retention expiration? Does the vendor have a standard Business Associate Agreement and experience in negotiating these types of contracts?

- **Inquire About Their Health Information Management and Closing Practice Expertise.** To ensure your patients' information will be protected but readily accesible, be sure to qualify the vendor's records management knowledge and healthcare-specific expertise. How many patient records do they manage? What healthcare facilities across the country do they work with? Have they ever supported a closed practice records management program before?

- **Consider Patient Care.** Patients may not be familiar with the process of requesting records from a third party. Does the records management vendor have dedicated teams with experience in Release of Information to assist your patients through the authorization and fulfillment process? Can the vendor ensure patients will receive their records in a timely manner? Will there be any costs to the patient for receiving copies of their records?

- **Identify What Information Formats and Types They Store and Manage.** Information no longer resides strictly on paper. It lives in digital format in your EMR, radiology, mammography and other systems. When evaluating alternatives to support the management of your critical records after your practice closes, inquire about the experience the provider has managing information in a variety of formats. For example, how can they help you cost-effectively manage electronic medical records while protecting them from security and cyber threats? Do they offer solutions to store other types of records such as X-ray films, lab specimens or medical images? Keep in mind, records come in all formats – and your plan must account for the storage, management and security of each.

- **Evaluate Capabilities Across the Full Information Management Lifecycle.** Your closing plan must make the appropriate accommodations to protect PHI at each stage of the information lifecycle. Just as important as protecting the information in storage or in transit, is the ability to securely destroy PHI upon retention expiration. This ensures HIPAA compliance and protects you from risks such as litigation, unauthorized access or future data breaches. Be sure to ask your records management provider about how they protect information at each phase of the lifecycle. Inquire specifically about how they track record retention to facilitate destruction upon expiration. It's also important to discuss how they are able to address the various systems or equipment that store PHI to ensure it is permanently removed or destroyed. Whenever possible, ask specifics about the destruction workflow processes and require that a certificate of destruction be generated as proof.

CONCLUSION

Creating a go-forward medical records management program to ensure compliance once your doors are shut for good can be a daunting task. Dropping the ball on any one part of that program – patient notification, e-record strategy, routine destruction – can put you at significant legal and financial risk.

Avoid potential disaster, and much unnecessary hassle, by partnering with a single vendor who can work with you to create an enduring medical record management program. Look for a vendor a knows healthcare information inside and out, who fully understands the demands of HIPPA compliance, who can store anything from a patient file to a medical specimen and who can manage your records through the entity of their lifecycle – from use to access to destruction. Choosing a capable vendor means your, and your patients', information is safe and accessible, and you are protected from risk.

FOR MORE INFORMATION ON CLOSING PRACTICE RECORDS MANAGEMENT CHECK OUT IRON MOUNTAIN'S "CLOSING YOUR PRACTICE CHECKLIST"

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated® (NYSE: IRM) is the global leader in storage and information management services. Trusted by more than 220,000 organizations around the world, Iron Mountain's real estate network comprises more than 85 million square feet across more than 1,400 facilities in 46 countries dedicated to protecting and preserving what matters most for its customers. Iron Mountain's solutions portfolio includes records management, data management, document management, data centers, art storage and logistics, and secure shredding, helping organizations to lower storage costs, comply with regulations, recover from disaster, and better use their information. Founded in 1951, Iron Mountain stores and protects billions of information assets, including critical business documents, electronic information, medical data and cultural and historical artifacts. Visit www.ironmountain.com for more information.

XXXX-SB-XXXXXXA