How to Transfer Medical Records Between Doctors Safely

July 10, 2025
By Michael H. Cohen

When a medical clinic is sold or merges with another practice, one of the most critical and legally sensitive tasks is transferring patient medical records. These records contain protected health information (PHI) and must be handled with strict compliance with HIPAA and state privacy laws.

The process of transferring patient medical records requires a structured protocol, typically involving data encryption, secure health IT systems, written patient notifications, and signed authorizations where necessary. If clinics fail to meet legal and ethical standards, the consequences can be severe, ranging from patient care disruptions to lawsuits, regulatory penalties, and loss of licensure.

This post will cover your legal obligations when transferring medical records. It will also let you know who can and how to transfer medical documents.

When Are Clinics Required to Transfer Medical Records?

Clinics are required to transfer medical records in several key situations where continuity of care or legal compliance is at stake. One of the most common scenarios is during a **merger, acquisition, or sale of a medical practice**. In these cases, patient records must be securely handed over to the new provider to maintain care and comply with HIPAA requirements.

Similarly, **when a physician retires, relocates, or otherwise leaves the practice and another doctor assumes responsibility for patient care**, the medical records must be transferred appropriately. Transfers are also necessary in cases of **medical group restructuring, hospital consolidation, or the dissolution of a practice**, where patient care responsibilities shift between providers or entities. In each of these cases, the transfer process must be handled with strict attention to legal and ethical standards to protect both the patients and the healthcare providers involved.

What Happens if Your Clinic Mishandles Medical Record Transfers?

Mishandling the transfer of medical records can have serious legal, financial, and reputational consequences. One of the most immediate risks is **violating the Health Insurance Portability and Accountability Act (HIPAA**), which strictly regulates how protected health information (PHI) must be managed and transferred. Non-compliance can lead to investigations, enforcement actions, and steep civil penalties, even if the violation was unintentional.

Beyond regulatory consequences, clinics may also face **lawsuits from patients** if their data is mishandled or privacy is breached during the transition. These claims can be costly and damaging to your practice's credibility. In some cases, mishandling medical records can also result in a **loss of trust from patients and peers, reputational harm in your community, and increased scrutiny from medical boards and regulatory agencies.**

In addition to legal penalties, your clinic could **lose critical payer relationships**, including Medicare or private insurance contracts, if your compliance failures are deemed substantial. For practices undergoing a merger or sale, this could jeopardize the entire transaction.

The best way to avoid these outcomes is to work with experienced healthcare attorneys who understand the legal nuances of record transfers and HIPAA compliance.

What Are Your Legal Obligations When Transferring Medical Records?

Transferring medical records between doctors or healthcare organizations isn't as simple as forwarding files to a new provider. It's a legally sensitive process governed by federal law, state regulations, and professional standards, all designed to protect patient rights and ensure the secure handling of private health information. Whether the records are in paper form or part of an electronic health record (EHR) system, the process must follow specific rules under the Health Insurance Portability and Accountability Act (HIPAA) and other relevant laws.

Healthcare providers also have a duty to ensure that any transfer of medical history or health records is done securely, only for lawful purposes, and with proper authorization or implied consent in the context of continuity of care. Failing to meet these obligations can lead to serious compliance violations and loss of patient trust.

HIPAA Requirements

HIPAA, or the Health Insurance Portability and Accountability Act, is the cornerstone of privacy and security compliance when transferring personal health information (PHI) between covered entities. **Under the HIPAA Privacy Rule, healthcare providers must protect patient information during every step of the transfer process, whether the request comes from the patient, a personal representative, or another doctor's office taking over care.**

The HIPAA Privacy Rule includes the "minimum necessary" standard, which requires healthcare providers to disclose only the minimum amount of patient information needed to accomplish the intended purpose. For example, if a patient is referred to a new doctor, only the relevant portions of their health records should be transferred, not their entire medical history, unless required for treatment.

When transferring electronic health records, providers must maintain an audit trail. This involves logging who accessed or transmitted the patient's data, when it occurred, and for what purpose. These logs are crucial for compliance and can serve as documentation if the provider is ever audited or must respond to a records request.

In most cases, transferring medical records for the purpose of treatment does not require formal written authorization. HIPAA allows an implied consent exception for continuity of care between providers. However, if the request is coming from an insurance company, lawyer, or non-treatment-related third party, a signed release form or written patient authorization is required.

State Laws

In addition to federal HIPAA requirements, state laws also govern the transfer of medical records, and these can vary significantly. Some states impose stricter privacy protections, extended retention periods, or more detailed records release protocols.

For example, California and Texas have additional privacy requirements that go beyond the federal law, including notification duties and limits on the use of sensitive health data. Healthcare organizations must understand both HIPAA and their specific state's medical privacy regulations to remain compliant.

State medical boards and laws often determine how long medical records must be kept before they can be destroyed. In many states, healthcare providers must retain records for at least 7–10 years. When a patient or new provider submits a records request, there must be a clear process for verifying identity, collecting proper forms, and responding within mandated

timeframes, typically within 30 days under HIPAA.

Other Regulations (Where Applicable)

Other laws may apply depending on the nature of the data and the method of transfer. For example, the HITECH Act (Health Information Technology for Economic and Clinical Health Act) expands HIPAA's scope for electronic health records, including breach notification requirements and enhanced patient rights to access their data. Additionally, state medical boards may have specific rules about how and when providers must notify patients or transfer information in the case of practice closure or provider retirement.

Do You Have to Notify Patients About Record Transfers?

Yes, healthcare providers have a legal and ethical obligation to notify patients when their medical records are being transferred to another doctor or healthcare organization, especially in situations involving a practice sale, merger, closure, or provider retirement. Under the HIPAA Privacy Rule, while patient authorization is not always required for transfers made for treatment purposes, patients must still be informed when there is a change in the custodianship of their health records.

Notification ensures patients are aware of who now has access to their private health information, how it will be used, and what rights they have regarding that information. It also supports the broader principle of patient autonomy and transparency in healthcare.

Clinics should notify patients as early as possible, ideally at least 30 days in advance of the transition. Accepted methods of communication may include mailed letters to the patient's last known address, secure patient portal messages, emails (if consented to), and notices posted in the clinic or on its website.

The patient notice should clearly explain that the clinic is undergoing a change (such as new ownership or the doctor's retirement), who will be responsible for maintaining the patient's medical records moving forward, how records will be handled (e.g., stored, transferred, or archived), and how patients can request copies or transfer their records to a provider of their choice. The notice should also include a mailing address or contact information for submitting a records request, along with deadlines or instructions for any follow-up.

Failing to notify patients properly can lead to legal and regulatory consequences, including HIPAA violations, patient complaints, loss of goodwill, and in some states, disciplinary actions from medical boards. In the event of a dispute, poor or absent communication about records transfers could also expose a practice to liability for abandonment or privacy violations.

What Is The Process of Transferring Medical Documentation?

Whether transferring paper records or electronic health records (EHRs), the process begins with a formal records request, either from the patient, a new provider, or another covered entity. The healthcare provider or administrative team must verify the identity of the requesting party, review any required release forms, and document the request. For transfers initiated due to a change in care, such as a new doctor taking over treatment, HIPAA allows the disclosure of private health information (PHI) without separate authorization under the treatment exception.

The step-by-step process typically includes:

1. Verifying the patient's identity or authorization via a valid release form.
2. Identifying the receiving doctor's office or healthcare provider.
3. Preparing the medical history or health records for transfer, limiting data to the minimum necessary unless required for ongoing treatment.
4. Logging the date, content, and method of the transfer for compliance tracking.

5. Delivering the records securely, either through physical mailing address using certified mail or electronically through an encrypted EHR system.

The role of EHR systems is critical in modern record transfers. These platforms streamline access, improve data security, and ensure that healthcare providers can deliver continuity of care efficiently.

However, even when using an EHR, practices must have the proper Business Associate Agreements (BAAs) in place with any third-party vendors who handle PHI. These agreements are required under federal law and confirm that the business associate will safeguard the data in compliance with HIPAA. Without a valid BAA, any involvement of outside vendors in storing, accessing, or transferring health records could be considered a HIPAA violation, putting your clinic at serious legal risk.

Who Can Transfer Medical Documentation?

Only certain individuals are authorized to initiate the transfer of medical documentation. **This typically includes the healthcare provider, designated administrative personnel, or a properly appointed personal representative acting on behalf of the patient.** The process must always protect the patient's health information and honor their rights under the HIPAA Privacy Rule and the Portability and Accountability Act.

Why Hiring a Healthcare Attorney Is Essential

Given the complexity of transferring medical records, the involvement of federal law, state-specific privacy rules, and the use of electronic health systems, hiring a knowledgeable healthcare attorney is essential. An experienced lawyer **can help you interpret the HIPAA Privacy Rule, manage compliance across jurisdictions, and prevent violations that could result in fines, lawsuits, or loss of your insurance contracts.**

One of the attorney's primary roles is to **create or review Business Associate Agreements**, ensuring that any third-party vendors, cloud-based services, or software platforms used in the transfer process are fully compliant with federal and state law. They can also assist with **drafting patient notices**, helping you inform individuals about how their patient information is being used and where it's going.

During mergers, acquisitions, or provider transitions, an attorney **ensures all aspects of the transfer of medical records are addressed**, including due diligence on data handling, reviewing forms, clarifying access rights, and preventing liability exposure. They also **help clinics maintain the necessary documentation** to defend their practices during audits or inquiries from state boards or federal regulators.

Need Help Ensuring HIPAA-Compliant Record Transfers?

Transferring medical records between doctors, practices, or healthcare organizations is a legal obligation that directly impacts patient care, privacy, and your clinic's reputation. From complying with the HIPAA Privacy Rule and the HITECH Act to meeting state-specific regulations and maintaining secure audit trails, every step of the process must be handled with precision.

Improper handling of medical documentation can result in costly HIPAA violations, lawsuits, regulatory penalties, and loss of trust from patients and payers. That's why it's essential for clinic owners, physicians, and healthcare systems to work with experienced legal counsel when planning or executing any medical record transfer. Whether you're facing a clinic sale, a provider departure, or a group restructuring, the right legal partner can help you stay compliant, reduce risk, and protect your practice.

FAQs

Do Clinics Need Patient Consent to Transfer Medical Records?

In most cases, patient consent is not required when records are transferred for treatment purposes, such as continuity of care.

However, if the transfer is for other reasons, like insurance or legal requests, written patient authorization is typically required under HIPAA.

How Should Medical Records Be Transferred Securely?

Medical records should be transferred using encrypted electronic health record (EHR) systems or secure mail with proper tracking. Unencrypted email or unsecured methods violate HIPAA regulations and put patient data at risk.

How Long Do Clinics Have to Retain Patient Records After a Sale?

Retention periods vary by state, but most require clinics to keep patient records for at least 7 to 10 years after the last date of service. Pediatric records may need to be kept longer, depending on state law.

Can Medical Records Be Transferred Without the Patient's Knowledge?

Yes, if the transfer is for treatment purposes, HIPAA permits it without explicit patient notification. However, patients should still be informed of changes in care or record custodianship as a best practice.

Can You Transfer Medical Records to a New Doctor?

Yes, patients have the right to request that their medical records be sent to a new provider. Clinics must comply with this request within a reasonable time frame, typically 30 days under HIPAA.

How Can I Transfer Medical Records to a New Doctor?

Submit a written records request or release form to your current provider, including the name and contact information of the new doctor. The current provider will then send the necessary records securely.

Who Has Ownership of Health Care Records?

Healthcare providers or facilities legally own the physical or electronic medical records. However, patients have the right to access, review, and obtain copies of their personal health information under HIPAA.