Are You Violating Patient Confidentiality?

John G. Classé, OD, JD

Please answer the following four questions BEFORE the lecture.

Question 1. Sale of a practice by the optometrist

If an optometrist sells a practice and its patient records to another optometrist, the seller’s ETHICAL obligation to protect the confidentiality of the records sold:

a. ends with the sale.
b. only ends with the sale if the buyer complies with HIPAA requirements.
c. continues past the sale only if the seller agrees to assume future responsibility.
d. continues past the sale for 6 years, then ends.

Question 2: Termination of associate’s employment in a private practice

When an employee optometrist leaves a private practice, ETHICALLY the employee:

a. has a continuing obligation to respect the confidentiality of patient information.
b. only has an obligation to respect confidentiality for the records of patients actually examined by the employee and not to the employer’s other patients.
c. must continue to respect confidentiality only if required to do so by the employment contract.
d. is no longer obligated to protect the confidentiality of patient information.

Question 3: Sale of interest by the co-owner of a private practice

If an optometrist sells all ownership interest in a partnership practice, what is the practice’s ETHICAL obligation to provide confidential information from the patient records afterwards?

a. If the optometrist requests patient information, the practice is required to provide it.
b. The practice has no responsibility to provide patient information from the records to the optometrist.
c. Information can only be given by the practice to patients, not to the optometrist.
d. If patients ask that information be transferred to the optometrist, the practice must comply.

Question 4: Office lease agreement requiring records transfer at termination

If an independent practitioner optometrist must agree at the termination of the office lease to leave the patient records to a future optometrist to be selected by the leasing company, ETHICALLY:

a. the optometrist can transfer them in this manner because the optometrist owns the records.
b. the records can be left behind as long as an optometrist eventually takes possession of them.
c. this requirement breaches confidentiality because the optometrist is obligated to transfer patient records to a successor practitioner who agrees to respect confidentiality.
d. the records cannot be transferred to another practitioner without a written sales agreement.

The answers to these questions will be discussed during the lecture.
Confidentiality and Patient Records

Significant legislation and litigation has been devoted to the issue of confidentiality of medical records. These legal actions have altered the manner in which patient information is collected, safeguarded, and disseminated. Failure to adhere to legal requirements can lead to lawsuits, fines, civil actions, and disciplinary sanctions.

Key legal and ethical issues to be discussed include:

- Federal privacy legislation for records
- Example state laws and board rules regulating the release of information in medical records
- Recent records litigation (breach of confidentiality)
- Ethical obligations when medical records are transferred
- Ethics-related legal action (unprofessional conduct)
- Contractual provisions will be reviewed in which legal and ethical issues related to confidentiality and records arise

Legal Considerations

A practitioner in private practice is the owner of patient records, but a “crazy quilt of federal and state laws” regulates the release of patients’ health care information. The most recent and far-reaching law in this regard is the Health Insurance Portability and Accountability Act (HIPAA).

The HIPAA provisions apply to:

- Health care providers
- Health care plans
- Managed care organizations
- Health care “clearinghouses” (entities that standardize health information—e.g., a billing service that processes or facilitates the processing of data from one format into a standardized billing format)

HIPAA also applies to business associates. Contracts are required for business associates and they are subject to HIPAA privacy provisions. If a business associate breaches HIPAA requirements, the practitioner is not responsible as long as there is a business contract with the associate that requires adherence to HIPAA.

Under HIPAA a practitioner is allowed to disclose patient information without consent in order to get paid, provide care, consult, refer or perform “health care operations”. Activities that are necessary to maintain and monitor care constitute “health care operations”: conducting quality assessment and improvement activities; developing clinical guidelines; performing case management; reviewing the competence or qualifications of health care professionals; providing education and training of students.
and practitioners; operating fraud and abuse programs; initiating business planning and management; and, importantly, selling or otherwise transferring patient records.#

HIPAA requires health care providers to notify patients in writing of the privacy policy of the practice regarding protected health information and to retain acknowledgements of receipt (a “privacy notice”, which is signed by the patient).

The rules also allow disclosure of personal health care information to third parties with the patient’s consent (an “authorization”, which must be in writing and describe the disclosure and the purpose for it).

The HIPAA Privacy Rule states that when protected health information is used or disclosed, only the information that is needed for immediate use or disclosure (the “minimum” necessary) should be divulged by the health care provider. This limitation applies to uses and disclosures for payment, treatment, or health care operations, or to disclosures that a patient has specifically authorized.

HIPAA addresses the transfer of patient records as part of the sale or closure of a practice: a practitioner is allowed to transfer by sale or other disposition patient records to a successor practitioner, as long as that practitioner abides by HIPAA requirements to respect confidentiality.* This requirement eliminates the need to personally notify all patients affected by the transfer.

Penalties for violation of the HIPAA privacy rules range from civil fines up to $100 per violation to fines as high as $25,000 for multiple violations within a year.

In a 2008 case, a Washington-based hospice and home care company allowed backup tapes, optical disks, and laptops, all containing unencrypted electronic protected health information, to be removed from the company’s premises over a six month period and left unattended. The media and laptops were subsequently lost or stolen, compromising the protected health information of over 386,000 patients.

The Department of Health and Human Services (HHS) brought an action against the company for HIPAA violations, fining the company $100,000 and requiring revision of the company’s policies and procedures regarding physical and technical safeguards (e.g., encryption) of off-site transport and storage of electronic media containing patient information; training of company members on the safeguards; periodic audits and site visits of the company facilities; and submission of compliance reports to HHS for a period of three years.

---

# The HIPAA requirement is as follows: “Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions…§ 164.501(6) (iv): The sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity”; Federal Register of March 27, 2002

* 65 FR at 82652: “We clarify in the definition of health care operations that a covered entity may sell or transfer its assets, including protected health information, to a successor in interest that is or will become a covered entity."
If it is determined that health information was “knowingly” and “wrongfully” disclosed, the complaint can be turned over to the Department of Justice as a criminal violation, and fines as high as $500,000 and prison time of up to 10 years can be imposed for malicious use of records.

HIPAA also regulates the destruction of records.

Paper containing sensitive information should be shredded or burned. Destruction can be performed in "distributed" fashion (e.g., by small shredders located near desks), or at a central location.

Removable magnetic disks (floppy, ZIP disks) and magnetic tapes (reels, cartridges) can be "degassed". "Fixed" internal magnetic storage (such as computer hard drives), can be cleansed by a re-writing process using software that over-writes the usable storage locations. Removable "solid state" storage devices ("flash drives") can also be cleansed by overwriting.

In addition to HIPAA, all jurisdictions have laws or judicial decisions that require practitioners to respect the confidentiality of information contained in patient records. For example, in California the state legislature has enacted the “California Confidentiality of Medical Information Act” (*California Civil Code*, Sections 56 through 56.37); this law provides for civil penalties and administrative fines for violations.

Section 56.101 of the statute holds that:

> “Every provider of health care…who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care…who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall be subject to the remedies and penalties provided…”

This law thus allows a legal action against a practitioner for negligently maintaining or destroying records. It is likely that other state laws enacted in other jurisdictions will follow this example.

In several states optometry board rules or regulations require practitioners to maintain records for a minimum period of years, but there is no specific requirement under the Texas Optometry Act or the state board rules. The Texas Optometry Board does comment, however, that practitioners should observe the 6 year period required by HIPAA for “notices, restrictions requests and information release”, the statutes of limitation for liability lawsuits (2 years for adults, and for minors if the injury occurs before age 18 by the minor’s 20th birthday), record retention requirements established by third party providers for audits, retention periods that will satisfy the IRS (generally 3 years), and the 4 year period that is established by the Texas Board of Optometry for
disciplinary actions filed against practitioners for violations of the optometry law or board rules. Judicial decisions have also contributed to the enforcement of confidentiality requirements. In a growing number of states, courts have recognized a cause of action for breach of the duty to respect confidentiality. In these jurisdictions a practitioner may be held liable for the release of confidential information, even if truthful, in a civil action for damages brought by a patient.

In a 2006 decision, an Illinois court determined that a medical employee’s responsibility to respect confidentiality was not limited to working hours but rather extended “to all times and to all places. In effect, for purposes of patient confidentiality...[a medical employee] is on duty 24 hours a day, 7 days a week.” *Bagent v. Blessing Care Corporation, et al.*, case number 04L8, Appellate Court of Illinois, 4th District, filed March 3, 2006. In this case, the court stated that an employer may be held responsible for an employee’s breach of confidentiality, even one which occurred in a “public tavern”, commenting that “an employee entrusted with confidential information in the course of his or her employment has a duty not to disclose the information—without limitation as to time or space” and that “the duty not to do so is actuated by the needs and requirements of the employer.”

Legal violations of confidentiality based on statutes or on optometry board rules or regulations, or on judicial decisions or interpretations, are not the only issues facing practitioners. Although ethical issues are not as frequently relied upon for enforcement of violations of confidentiality, they provide a potential source of disciplinary action and thus must also be considered.

**Ethical Considerations**

Ethical rules do not have the force of law but are usually incorporated into state practice acts as legal obligations, and violations (for “unprofessional conduct”) can result in disciplinary action (including loss of license) for a practitioner.

In a 2001 case, a New Jersey physician charged with not cooperating with the medical board’s investigation had his license suspended for 2 years and was fined $2,500 for, in part, leaving confidential patient medical records unsecured and unprotected at a gas station, where they were to be picked up by an investigator from the state’s Division of Consumer Affairs Enforcement Bureau.

Some states have adopted ethical rules as part of their optometry board rules or regulations, again by describing acts that constitute “unprofessional conduct”. But few ethical rules, statutes, or board rules or regulations specifically address the transfer of patient records by optometrists.

However, ethical situations involving records occur regularly: when a practice is sold to a successor provider; when an associate’s employment ends; when a partner leaves a private practice; and when an independent contractor’s office lease agreement terminates.
From an ethical standpoint, the key consideration is to accomplish the records transfer in a manner that preserves the confidentiality of the health information.

Although this obligation is effectively transferred to a successor provider when *ownership* (not mere possession) of the records is transferred, if the circumstances of the transaction do not result in protection of confidentiality, then both providers may be held to have breached ethical requirements.

Similarly, a transfer of *possession* does not relieve the transferring provider of ethical obligations to preserve confidentiality. If confidentiality of records is breached by the provider in possession, responsibility for the breach may also be imposed upon the transferring provider because ownership of records confers both an ethical and a legal obligation to protect confidentiality, even if the records are in the possession of another provider.

Because of the importance of patient records in preserving continuity of care, when there is a change of provider the transfer of records is a key part of the transaction, and confidentiality of patient records and information should be described in writing within the contract that constitutes the agreement between the parties.

**Examples from Contracts**

Four actual contractual provisions will be reviewed to illustrate how confidentiality requirements must be managed when ownership or possession of records is transferred.

**Example 1: Sale of a practice to a successor practitioner**

An optometry practice sales contract contains the following provisions:

**Seller hereby irrevocably appoints Buyer custodian of all Seller's patients' records.** In the event Buyer considers any of the records no longer useful (inactive), Buyer shall provide written notice to Seller or his/her representative specifying the names of the records to be returned then allowing thirty (30) days for Seller's written instructions as to what to do with the records. If Seller does request possession of the records, he/she shall pay for pick-up or transfer of the records and if he/she does not request possession of the records, then Buyer can dispose of and destroy the records. In the event Seller requires any record for reason of suit against the Seller subsequent to the Closing Date of Sale, or for any other valid cause, Buyer agrees to furnish copies thereof at Seller's expense or allow Seller reasonable access to review such records.

Key question: Does a seller’s legal and ethical obligation to ensure that confidentiality is protected extend beyond the sale?

Legally, if a valid transfer of ownership is made, the duty to provide confidentiality becomes the buyer’s responsibility after the sale. An ethical breach could occur, however, if the transfer is of such character that protection of confidentiality could not be obtained afterwards.
Ethically, a seller of records should require that they be maintained and disposed of properly, even after sale, and the return of records that are to be destroyed to the seller by a buyer is both ethical and legal.

A HIPAA compliance clause should be included in the contract of sale to ensure that these obligations are part of the agreement (see Conclusion for example).

**Example 2: Termination of associate’s employment at a private practice**

The optometrist’s employment contract contains the following provisions:

All records, charts and personal files concerning the patients of Employer shall belong to and remain the property of Employer. On termination of his employment, Employee shall not be entitled to keep or reproduce the names or addresses of patients or to keep or reproduce Employer’s records, charts or files related to any patient unless the patient shall specifically request that his records be transmitted to Employee.

Key question: Does an employee who leaves a private practice have a continuing legal and ethical obligation to protect confidentiality even though the records belong to the employer?

Legally and ethically, the responsibility for protecting confidentiality belongs to the employer, because the employer is the owner of the records. However, an employee is also legally and ethically bound to ensure confidentiality while working for the employer.

After the employment has ended, responsibility for protecting the confidentiality of the records remains with the employer. Even though the ex-employee does not have ownership or possession of the records, however, there remains a legal and ethical obligation to maintain the confidentiality of patient information, just as for the employer. If patient records (or copies) are actually transferred to the ex-employee, the responsibility to preserve confidentiality is joint.

**Example 3: Sale of ownership interest by a practitioner in private practice**

The business entity’s operating agreement states that:

Upon dissolution of the partnership, the parties agree as follows:

All patient records belonging to each partner prior to the execution of this agreement shall remain the exclusive property of each of the partners, and all new records—those coming into the partnership following the execution of this agreement—shall be treated in such a way that each of said patients will be notified of the dissolution so that the patients shall have a choice of whichever doctor they elect to continue with for future treatment and service.

Key question: What legal and ethical responsibility does a practice business entity have to protect the confidentiality of records after the partner leaves?

A practitioner who sells an ownership interest in a business entity is no longer legally or ethically bound to protect the patient records owned by and in the possession of the
business entity but does have an ethical responsibility to respect the confidentiality of the information contained in them.

The departing practitioner also assumes both a legal and an ethical responsibility to preserve the confidentiality of any records (or copies) taken from the business entity.

When a business entity (general partnership, limited liability company, professional association or corporation, subchapter S corporation) is granted ownership of patient records, the entity is responsible for the protection of confidential information, and if records are provided to practitioners the entity must assure that the practitioners will similarly respect confidentiality. This same obligation extends to copies of patient records provided to practitioners.

For this reason it is appropriate for practitioners who leave and receive records (or copies) to sign a statement agreeing to adhere to HIPAA confidentiality requirements.

**Example 4: Termination of an office lease by an independent contractor**

The office lease agreement for an optometrist contains the following provisions:

Unless prohibited by applicable state or federal requirements, and subject to such requirements, Optometrist shall, immediately upon request by LESSOR, deliver complete copies of all patient records and files relating to Optometrist's practice in the Clinic Premises to any licensed optometrist LESSOR may designate.

The optometrist to whom copies of such records are delivered shall protect the confidentiality of such records.

LESSOR and Optometrist acknowledge that such delivery of copies of patient records and files is intended solely for the convenience of patients who may wish to receive optometric services from a successor optometrist at the Clinic Premises.

Key question: Can an independent contractor legally and ethically agree to transfer patient records as a condition of signing a lease agreement for an office?

An independent contractor owns the records of patients seen, and can legally assign them (or give copies) to a successor practitioner.

If the successor practitioner is not known at the time the transfer is agreed to, however, it is impossible for the independent contractor to determine if the successor would comply with HIPAA confidentiality requirements, which would make the transfer illegal and unethical. Such a transfer to an unknown successor, once made, would not relieve the independent contractor of responsibility for protection of confidentiality.

If at the end of the lease the independent contractor transfers ownership of records to another practitioner who is HIPAA compliant, the transfer would not be unethical since the practitioner would protect confidentiality.
If the independent contractor merely assigns possession to an optometrist who is HIPAA compliant (such as an optometrist or physician), the transfer would not be unethical but there would continue to be a joint responsibility to protect confidentiality.

If the independent contractor takes copies of the records and leaves the originals with a HIPAA compliant optometrist, or takes the original records and leaves copies with a HIPAA complaint optometrist, a joint responsibility to safeguard confidentiality would continue.

**Conclusion**

Legal and ethical responsibilities to protect confidentiality are assumed whenever patient records are compiled by a practitioner, and can only be transferred when a successor practitioner agrees to assume them.

The practitioner to whom records are transferred must agree to comply with HIPAA confidentiality requirements. This agreement is best obtained in writing.

A HIPAA compliance statement for a records transfer should contain language similar to the following:

*It is acknowledged by both parties that the transfer of ownership of the medical records and files by Seller to Buyer will be conducted in accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA).*

*Buyer is a “covered entity” as defined by HIPAA, and agrees to comply with the HIPAA Privacy Rule to protect the confidentiality of individually identifiable health care information for all medical records and files transferred from Seller.*

*Buyer agrees to adhere to HIPAA security requirements for medical records and for individually identifiable health care information and to thereby prevent breaches of confidentiality.*

*Buyer will comply with federal medical record maintenance requirements and those of this State as they pertain to optometrists, and in addition will ensure that the medical records and files transferred to Buyer will be kept for a minimum of 6 years, as required by HIPAA.*

*Buyer will comply with federal and state legal requirements for the destruction of records and files transferred from Seller under this agreement.*

If an ethical transfer is not made, the practitioner’s responsibility to protect confidentiality is not relieved, and a subsequent breach of confidentiality may subject the practitioner to legal sanction.