AMERICAN ACADEMY™
OF OPHTHALMOLOGY

ADVISORY OPINION OF THE CODE OF ETHICS

Subject:	Release and Confidentiality of Patient Records
Issues Raised:	What are the ethical and related obligations concerning medical records and the release of patient information?
Applicable Rules:	Rule 1. Competence Rule 4. Other Opinions Rule 14. Interrelations Between Ophthalmologists Rule 17. Confidentiality

Background

Although the law varies from state to state, as a general rule, a physician, a physician's clinic, or group practice owns medical records, subject to the doctor-patient privilege and the patient's expectation and right of privacy. The information within the medical record is considered the property of the patient, and the patient has an ethical right and, generally, a legal right to complete and timely access to this information. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 provided regulation of the security and privacy of medical data. Every practitioner is required to be familiar with this law. Ownership of patient medical records is also subject to the patient's right to obtain copies of those records or to have copies transferred to another person. Most states provide for an exception, excusing a refusal to deliver medical records to a patient if it is determined that information in the records could be detrimental to the physical or mental health of the patient or is likely to cause the patient to harm themselves or someone else.

General Discussion

In order to provide quality medical care, it is essential that ophthalmologists cooperate fully, freely, and promptly in sharing copies of medical records. Medical records may include progress notes, prescriptions, charts, reports, laboratory results, and technical information used to assess the patient's health condition, as well as letters, photographs, X-rays, and diagnostic imaging. Reports and letters may contain wording that prevents release of that information. This is particularly true of consultants' reports. (It is important to note that a physician may also keep personal notes not related to patient care that are separate and distinct from the medical record; these do not have to be released.)

In most states, a physician may be subject to severe disciplinary action, including suspension or even revocation of licensure, for failure to comply promptly and fully with these requirements. Except for a recognized statutory reason (e.g., an improperly executed release), an ophthalmologist should not refuse to release a patient's medical records to the patient, the patient's legal representative, or another person upon receipt of proper authorization. In some instances, such as for patients with HIV, a special authorization may be required. Medical records should never be withheld merely because of an unpaid bill for services or because the patient has elected to see a competing practitioner. However, it is permissible in most states to bill for the reasonable costs of making the requested copies.

Compliance with HIPAA

Following the enactment of HIPAA in 1996, the federal government published medical records privacy regulations in December 2000 (modified August 2002). These regulations protect the privacy of individuals' identifiable health information by restricting the use and disclosure of such information. The federal government published regulations adopting standards for the security of electronic health information in February 2003. The security rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to ensure the confidentiality of electronic protected health information. The regulations for privacy and security of medical records are broad, and together the two sets of regulations cover electronic, paper, and oral communications when they include any individually identifiable patient information. Failure to comply with these regulations may result in penalties of $100 to $50,000 for *each violation*. The final amount will be determined by the extent of the violation, the nature and extent of resulting harm, and other factors, including knowledge of the law, reasonable cause, and willful neglect. The maximum penalty per calendar year for multiple violations of an identical provision of HIPAA is $1.5 million. It is critical, therefore, that practitioners become familiar with the HIPAA requirements related to medical records and always use, disclose, and safeguard individually identifiable patient health information in compliance with HIPAA and related regulations.

A new educational initiative, *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information* (launched by Office for Civil Rights [OCR] and the Department of Health and Human Services' [HHS] Office of the National Coordinator for Health Information Technology) offers health care providers and organizations practical tips on ways to protect electronic private health information (e-PHI) when using mobile devices. Mobile electronic devices, such as laptops, tablets, and smartphones, which are now used quite frequently in practitioners' offices, bring their own set of requirements if not currently required by electronic health record regulations. For example, practitioners must be aware of and act appropriately with respect to data back-up, mobile device disposal, security incident reporting, and mobile device passwords and encryption. Additionally, consideration must be given in e-communications between health care providers and patients with respect to e-mail authorizations, including whether e-mail communication is part of the confidential physician-patient relationship, accessibility to the communication at the practitioner's office and at the receiving end, and whether documentation of the communication becomes part of the patient record.

The following case study includes a selection of the problematic e-communication elements noted above and is a modification of an actual HIPAA violation.

Case Study

Dr. A, a private practitioner in a refractive surgery practice, received a notice of investigation from the OCR following the report of a breach of the HIPAA Security Rule. After reading the notice, Dr. A realized that a former employee reported him for failing to report the theft of an unencrypted, non-password-protected laptop that contained e-PHI for 771 patients from his office several months prior to her departure. Additionally, the report indicated that Dr. A's practice routinely had staff use their personal electronic devices to communicate about patients' e-PHI, including the discussion and in-office reporting of test results that were intended for inclusion in patients' medical records. Furthermore, the report indicated that unsecured laptops used for patient interviews were left in examination rooms, even when new patients were escorted into those rooms.

The notice from the OCR listed the following actions that had to be taken to rectify the faults found with Dr. A's HIPAA compliance: the practice must institute routine risk analyses to safeguard e-PHI; policies and procedures to address mobile device security as required by the HIPAA Security Rule; and required reporting of "impermissible use or disclosure of e-PHI"

per the Breach Notification for Unsecured Protected Health Information, issued pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act. Lastly, it must incorporate into its staff education procedures HIPAA's new educational initiative, *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information.*

The terms and conditions of the settlement reached between Dr. A and the OCR required (1) payment of a $50,000 fine, (2) payment of the government's costs associated with the investigation, and (3) completion of a Corrective Action Plan, which included creation of the procedural policies noted as lacking in Dr. A's practice in the initial notification of investigation. As a professional liability insured by Acme Insurance Company (or ABC Insurance Company), Dr. A was covered by Acme's cyber liability protection for the fine, his own legal expenses (including investigation costs), and the expense incurred in notifying patients of the breach.

Release and Confidentiality of Patient Records – Special Situations

Several specific situations with respect to the release and confidentiality of patient records require special attention. Ophthalmologists should be aware of federal rules (42 C.F.R. Part 2) concerning the confidentiality of patient records on alcohol and drug abuse. These rules prohibit the disclosure of this portion of medical records except under specific conditions. Violation of these rules is a federal crime.

First, the ophthalmologist should not release these records unless the patient executes a release form specifically covering alcohol and drug-abuse records. Second, when releasing copies of such medical records to anyone other than the patient, the ophthalmologist should place a cover sheet on all record sets stating the following, in this or substantially similar language:

Notice of Confidentiality

This information has been disclosed to you from records protected by federal confidentiality rules (42 C.F.R. Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug-abuse patient.

Laws governing the release of AIDS and HIV-related information vary greatly from state to state. In New York and Maine, for example, the regulations are stringent: AIDS and HIV-related information should only be released upon execution of a consent form specifically designed for that purpose; a general release form is not adequate. The form should be witnessed and should include a notice prohibiting redisclosure. Ophthalmologists should be aware of and comply with their individual state's regulations.

Transfer of Records to Another Practitioner

Another situation of potential concern involves the disposition of patients' medical records upon the death or retirement of an ophthalmologist or the sale of that ophthalmologist's practice. In many such instances, it is wrongly assumed that the records are freely transferable, and that the recipient has the same ownership rights as the original ophthalmologist. However, in many states the recipient may be only a custodian of the

patient's medical records and would have no right even to inspect those records except to obtain the patient's name and address for the purpose of communicating with the patient, unless and until the patient (1) expressly or by clear implication (as by seeking medical advice, prescription renewal, treatment, or other medical assistance from the new ophthalmologist) consents to the transfer of his or her medical records, or (2) properly directs the transfer of the records to another physician. If records are transferred, the receiving physician must retain the original physician's records in a secure place for the applicable time period required by state law for the retention of patient records. In addition, it is not unreasonable for the family or legal counsel of the deceased physician or the buyer of the practice to have a written agreement that the buyer or the executors of the deceased physician shall have access to copies of patient records to comply with inquiries of professional medical conduct proceedings or malpractice actions.

Applicable Rules

"*Rule 1. Competence*. An ophthalmologist is a physician who is educated and trained to provide medical and surgical care of the eyes and related structures. An ophthalmologist should perform only those procedures in which the ophthalmologist is competent by virtue of specific training or experience or is assisted by one who is. An ophthalmologist must not misrepresent credentials, training, experience, ability or results."

"*Rule 4. Other Opinions*. Ophthalmologists should be cognizant of the limitations of his/her knowledge and skills and be willing to seek consultations in clinical situations where appropriate. The patient's request for additional opinion(s) should be respected."

"*Rule 14. Interrelations Between Ophthalmologists.* Interrelations between ophthalmologists must be conducted in a manner that advances the best interests of the patient, including the sharing of relevant information."

"*Rule 17. Confidentiality.* An ophthalmologist shall respect the confidential physician-patient relationship and safeguard confidential information consistent with the law."

Other References

"*Principle 2. An Ophthalmologist's Responsibility*. It is the responsibility of an ophthalmologist to act in the best interest of the patient."

American Medical Association Code of Medical Ethics Opinions 3.3.1 ("Management of Medical Records"); 7.04 ("Sale of a Medical Practice"); and 1.2.3 ("Consultation, Referral and Second Opinions"). Available at: https://www.ama-assn.org/

Substance Abuse and Mental Health Services Administration, U.S. Department of Health and Human Services. 42 C.F.R. Part 2, "Confidentiality of Substance Use Disorder Patient Records." Available at: https://www.ecfr.gov/cgi-bin/text-idx?rgn=div5;node=42%3A1.0.1.1.2.

Federal Office of Civil Rights, Health Information Privacy. Available at: http://www.hhs.gov/ocr/privacy/.

Approved by:	Board of Directors, September 1989
Revised and Approved by:	Board of Directors, June 1992
Revised and Approved by:	Board of Trustees, February 1997
Revised and Approved by:	Board of Trustees, November 2003
Reaffirmed and Approved by:	Board of Trustees, March 2008
Revised and Approved by:	Board of Trustees, April 2016

Revised and Approved by: Board of Trustees, December 2021

P.O. Box 7424 / San Francisco, CA 94120 / 415.561.8500