

This material appeared as a section in the book, “The Biggest Legal Mistakes Physicians Make and How To Avoid Them”, Seak, Inc., 2005. Reproduced with permission.

The 10 Biggest Legal Mistakes Physicians Make That Could Result in a Violation of HIPAA

By Scott P. Sandroek, Esq.

Executive Summary

The Health Insurance Portability and Accountability Act (HIPAA) became effective August 21, 1996. One element under HIPAA was the creation of regulations to protect the privacy of personal health care information. The standards for privacy of individually identified health information (referred to as PHI) were initially proposed in 1999, were finalized in December 28, 2000, and subsequently amended on several occasions with the last amendment on August 14, 2002.

While physicians are already bound by the Code of Ethics to maintain the confidentiality of patient information and are subject to additional restrictions under various provisions of state law, HIPAA imposes additional obligations on physicians to provide a written notice of legal rights to patients, to comply with patient directives, and to restrict disclosure of information except as authorized by the patient or specifically exempted under HIPAA. Failure to comply can result in significant fines and penalties.

COMPLIANCE: HIPAA

Mistake 1 Failing to Give Patients a Copy of the Privacy Notice

Physicians sometimes believe that because patients may not understand the privacy notice or because patients often throw the notice away, that it is a waste to give them a multiple-page privacy notice. Some physicians believe that merely posting the notice in their lobby or expecting the patient to read one copy of it is adequate for compliance. The interpretive guides to the privacy rules clearly require the health care provider to deliver a copy of the privacy notice in its entirety to each patient at the time of the first office contact. Posting the notice or having patients read it without giving them a copy fails to meet those requirements.

Action Step Physicians should instruct their staff that each patient is to be given a copy of the privacy notice at the time of the initial office contact.

Mistake 2 Thinking That the Privacy Notice Is a “HIPAA Compliance Plan”

Physicians sometimes believe that as long as they deliver the privacy notice to the patient they have satisfied their HIPAA obligations. The regulations are clear that while the privacy notice is important, the physician has additional responsibilities: to have a formal policy, to designate a privacy officer, to develop procedures for the accounting of the disclosure of PHI, and to develop internal procedures to train staff to handle each component described under the privacy rules.

Action Step Physicians should engage experienced counsel to prepare and implement a detailed and thorough HIPAA compliance plan for their office.

Mistake 3 **Discussing the Patient’s Health Condition with Their Family Members**

Prior to HIPAA, physicians would routinely discuss with family members the condition of the patient. Under HIPAA restrictions however, physicians may not have that discussion without first receiving prior permission from the patient to identify which members of the family can receive PHI. The failure of physicians to pre-identify with the patient those who are able or authorized to receive the information can result in a significant HIPAA violation.

Action Step Physicians must pre-identify with the patient those whom the patient has authorized to receive his or her PHI.

Mistake 4 **Releasing Health Information to the Patient’s Employer without Having Obtained Written Authorization**

Physicians are often asked to sign forms concerning the health condition of employees, either to permit them to return to work or to show absence from work because of health conditions. While these practices are common, HIPAA imposes new responsibilities on physicians to not release such information without prior written authorization from the patient. Under the HIPAA regulations, there are clearly defined elements that must be in a HIPAA authorization form. The form must be executed by the patient (or an authorized agent of the patient, such as a power of attorney), and the form must be signed before the release of the information to the third party. These authorizations must be obtained in any situation in which the health information is released for purposes other than the treatment for the health condition of the patient or for the payment for the health care treatment.

Action Step For any release of information for use other than treatment or payment, the physician must obtain a HIPAA authorization in advance from the patient.

Mistake 5 **Releasing Information without Maintaining a Record of the Recipients of the Information**

In Mistake 4, physicians released information at the patient’s request but without the proper forms being signed. If the signed form is received, physicians must maintain detailed records of any incidence in which such release of information occurred. Under HIPAA, there is a responsibility of physicians to fully account for any release of information in a situation other than treatment or receiving payment for the care. For example, for each release of information to an employer, the physician must maintain in a separate record the date of release, the information released, and the person to whom it was sent. Under HIPAA, the patient is entitled, upon request, to a complete and accurate listing of any such disclosures. This accounting is not required for the routine release of information for the treatment of the patient or to secure payments, such as sending a billing slip to an insurance carrier.

Action Step Physicians must develop procedures to maintain an accurate and complete accounting of the release of any information outside of treatment or payment.

Mistake 6 **Refusing to Give Patients a Copy of Their Records**

Occasionally, patients may ask a physician for a complete copy of their records and the physician will decline to provide the records either because the patients have not paid their bill or because the records contain information that the physician thinks may be detrimental to the patient or to the physician. With the limited exception of information dealing with mental health issues (which have unique rules) under HIPAA, patients are entitled to a copy of their medical records and the physician is entitled to charge a reasonable copy fee for those records. Refusing to release the records or to provide a copy can result in a HIPAA violation.

Action Step Physicians are required to release records to a patient upon the patient's prior written request.

Mistake 7 Releasing Records Pursuant to a Subpoena or Letter from the Patient's Attorney

Physicians receive requests from attorneys representing patients in a variety of legal proceedings or occasionally receive subpoenas requesting medical records. Under HIPAA, physicians have a heightened obligation not to release medical records without prior written authorization from the patient. If the request comes from an adverse party, physicians may not release the records without obtaining a specific court order after first taking reasonable steps to obtain a qualified protective order from the court to limit the disclosure of the protected health information. Physicians are further required to edit the file to release only that portion of the medical records related to the injury or condition described in the request. Under the "minimum necessary standards," physicians may not release the entire medical file and are required to release only that portion of the file that is absolutely necessary.

Action Step Physicians should not release medical records simply pursuant to a request by an attorney or a subpoena, but should instead insist on written authorization or a specific court order.

Mistake 8 Releasing Test Results over the Phone without First Obtaining Security Clearance

Physicians run numerous tests and evaluate the condition of their patients. In communicating information, physicians are required to take reasonable steps to verify the identity of the person to whom such information is released. In many cases, the office may contact the patient by telephone and leave a message to call the office. When the patient returns the call, the office staff needs to take reasonable steps to confirm the identity of the person on the telephone (e.g., requesting unique identifiers such as the patient's Social Security number).

Action Step As part of the HIPAA compliance plan, medical staff should have a policy to require security identification before releasing medical information to anyone over the telephone.

Mistake 9 Failing to Have Computer Security Systems in Place

Older computer programs do not contain password protection or other security features. Even though the medical office may have a separate office space, the security regulations require physicians to implement reasonable security measures to prevent unauthorized access to electronic medical records. Those steps include using security passwords, restricting access, repositioning computer screens so that they are not accessible to the public, and other reasonable

steps that more modern versions of software programs would provide. Physicians must implement a policy mandating the use of security passwords, restrict computer access to essential personnel only, and otherwise verify security features for their computers and electronic information.

Action Step Physicians should develop a proactive security system for electronic records.

Mistake 10 Relying on Commercial Software That Have No Expressed HIPAA Compliance Warranties

Physicians have the responsibility to ensure compliance with HIPAA. A blind reliance on commercial software to meet their obligations may not be enough. Physicians should require as a condition of any purchase or license of software that they obtain an expressed warranty by the software vendor that the software is fully compliant under HIPAA and that the vendor will update the software to meet the ongoing changes and corrections in the reporting requirements.

Action Step Physicians should obtain a written affirmative warranty from vendors of their compliance with HIPAA, including an indemnification of damages to the physician.

Conclusion

Physicians should work with experienced health care legal counsel to develop and implement a comprehensive HIPAA compliance plan for their medical practice. Reliance on prepackaged material or the failure to pay attention to training can lead to errors and omissions resulting in liability to the physician.

About the Author

Scott P Sandroek, Esq., is a partner at Brennan, Manna & Diamond, LLC in Akron, Ohio and has more than 25 years of experience in representing physicians and medical groups in health care, corporate, and regulatory issues. Sandroek can be contacted by telephone at 330-253-4367 or by e-mail at spsandroek@bmdllc.com.