Protecting the Patient's Right

Privacy When Responding to Subpoenas for Medical Records

Healthcare providers are charged with protecting a patient's right to privacy when disclosing protected health information (PHI), but how is that accomplished when the provider is faced with responding to a federal subpoena for medical records without a patient authorization?

The answer is simple if a provider understands its obligations and liabilities under the law and exercises due diligence when answering such legal requests.

The Subpoena Power

Subpoenas are routinely used by attorneys to obtain medical records from third parties for a variety of civil lawsuits, from personal injury to employment law to medical malpractice claims. The subpoena power comes from Rule 45 of the Federal Rules of Civil Procedure. Rule 45 allows a subpoena to command a provider to give oral testimony for deposition or trial purposes (known as a subpoena ad testificandum), command the production or inspection of documents and information (known as a subpoena duces tecum), or both. In the alternative, a subpoena may command the production or inspection of documents by a specified date in lieu of providing oral testimony. This article only addresses third party subpoenas for the production of documents. If you are subpoenaed to provide oral testimony or if you are subpoenaed as a party to a lawsuit, you should immediately contact an attorney.

Rule 45 requires a subpoena to specify the documents sought, the name of the issuing court, the title of the lawsuit and the civil action number, and the time and place for production or inspection of documents. Before the subpoena can be served on a provider, the issuing attorney is obligated to provide advance notice of the subpoena to all other parties to the lawsuit. The purpose of this rule is to

allow time for the parties to work out any objections regarding the validity or scope of the subpoena. Once a subpoena is served on a provider, the provider is required to produce the requested medical records on the specified date. However, the provider must be aware of its requirements under HIPAA since automatic compliance with a subpoena may constitute an unlawful disclosure of protected health information (PHI), placing the provider at risk for hefty fines and litigation.

The Interplay Between HIPAA and Subpoenas

The disclosure of PHI without a written authorization from the patient is generally prohibited under HIPAA, with a few limited exceptions. One of those exceptions applies to the disclosure of PHI pursuant to a valid subpoena. Specifically,

HIPAA permits disclosure in response to a subpoena if one of the following conditions is satisfied:

1. The provider must receive a written statement and accompanying documentation from the attorney issuing the subpoena demonstrating that:
   a. A good faith attempt was made to provide written notice of the subpoena to the patient or his or her attorney;
   b. The written notice included sufficient information to allow the patient to raise an objection to the subpoena;
   c. The time for objecting to the subpoena has passed; and
   d. The patient did not object to the subpoena or that any objections by the patient were adequately resolved by the court.

2. The provider must receive a written statement and accompanying documentation from the attorney issuing the subpoena demonstrating that:
   a. All parties to the lawsuit have agreed to a qualified protective order and have presented it to the court or that the attorney issuing the subpoena has filed for a protective order. A qualified protective order limits the use of the requested PHI to the lawsuit and requires the PHI to be returned or destroyed when the lawsuit ends.

3. The provider makes reasonable efforts to provide notice of the subpoena to the patient and the patient does not make any objections to the release of his or her PHI.

4. The provider obtains a signed HIPAA authorization from the patient for the release of the subpoenaed medical records.

These conditions can be found in Title 45 of the Code of Federal Regulations, Section 164.512(c)(1)(ii), (e)(1)(iii)-(vi).

Accordingly, a provider must take specific measures to protect a patient's right to privacy when responding to subpoenas for medical records. Upon receiving a subpoena, a provider should:

1. Immediately calendar the date on which the documents must be produced or inspected;

2. If the amount of time to respond is not adequate, then request an extension of time from the issuing attorney, making sure to document the request and approval in writing for your records;

3. Evaluate the subpoena against the HIPAA required documentation. If the information contained in the subpoena does not meet one of the listed HIPAA conditions, then it is incumbent upon the provider to obtain the necessary written documentation from the issuing attorney in a timely manner. In the alternative, the provider may contact the patient directly to obtain authorization.

4. The subpoena, accompanying documentation, and any written correspondences between the Provider and the issuing attorney should be retained in case of an investigation or audit.

Once a provider obtains the necessary written assurances, it must release the medical records on the date specified in the subpoena. In the event that the issuing attorney cannot produce the necessary documentation

Take Charge of Your Career—GET CERTIFIED!

CCS

AHIMA's highly-respected Certified Coding Specialist (CCS) credential demonstrates a practitioner's tested data quality and integrity skills, and mastery of coding proficiency. Our exam prep's are designed to serve as a valuable supplement to your overall education plan.

For more information on the CCS Credential, visit ahima.org/certification/CCS.

CCS Exam Prep Workshops

These workshops are designed to assist individuals in strengthening and reinforcing competencies needed to prepare for the CCS exam.

In-Person

April 1, 2016 | Chicago, IL
Product #: 16CCS04 | CEUs: 8
Price: $399 | Member Price: $299

June 3, 2016 | Chicago, IL
Product #: 16CCS10 | CEUs: 8
Price: $399 | Member Price: $299

Virtual Meeting Series

January 13 | January 20 | January 27 | February 3
Product #: 16VECCS101
Price: $399* | Member Price: $299*

Do these dates not work for you? There are several other virtual meetings throughout 2016. Check ahima.org/events to find the dates that work for you.

**Price is inclusive of all four dates listed.*

To register for meetings, visit ahima.org/events.

Online CCS Exam Prep

Coming Second Quarter 2016!

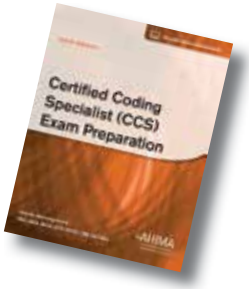
Watch for this virtual experience, designed as a valuable supplement to preparing for the CCS exam.

Book

***Certified Coding Specialist (CCS) Exam Preparation*, Sixth Edition**

Product#: AC400414
Price: $79.95
Member Price: $64.95

To purchase, visit ahimastore.org



AHIMA
American Health Information Management Association®

136.15

or if the patient does not allow the provider to make the disclosure, then the provider is simply not authorized to disclose the subpoenaed medical records. In this case, the provider should immediately contact an attorney, as it will need to object to the subpoena in writing, detailing the reasons for its objections, including the documentation needed to comply with HIPAA.

In addition to HIPAA, providers must be aware of and comply with their respective federal and state laws that provide heightened confidentiality for certain types of medical records before making any disclosures. For example, Title 42 of the Code of Federal Regulations § Part 2 limits the disclosure of drug and alcohol treatment records. And certain state laws may limit the disclosure of records relating to HIV/AIDS records, mental health records, and other sensitive records. Accordingly, a careful review of the medical records must be conducted to redact any such sensitive information prior to disclosure.

Subpoena v. Court Order

Despite its legal language, a subpoena signed by an attorney or a court clerk differs from a court order or subpoena that is signed by a judicial officer such as a judge or magistrate. The distinction is important because of the exceptions carved out by HIPAA. If a provider receives a court order or subpoena signed by a judge or magistrate, a court-ordered warrant, or grand jury subpoena, it must disclose the requested documents. Of course the provider must pay careful attention not to disclose more than what is expressly authorized by the document to maintain compliance with HIPAA.

Steps to Risk Mitigation

In order to minimize the risk of unlawful disclosures and to foster a culture of compliance, a provider should have policies and procedures in place that address disclosures pursuant to a subpoena. In addition, employees that are responsible for handling and responding to subpoenas must be trained on such policies and procedures.

Protecting your reputation as a provider by mitigating the risk of a government investigation initiated by a patient complaint that alleges his or her PHI was improperly disclosed is avoidable by having the proper policies and procedures in place, and ensuring they are followed.

(This article does not address subpoenas issued by state courts. And to the extent state law is more restrictive than HIPAA, state law controls, which may require additional steps to be taken before disclosing such information.)

Sheba E. Vine, Esq., is the Director of Regulatory Compliance at First Healthcare Compliance (www.1sthcc.com). In this role, Ms. Vine serves as an expert and resource for clients concerning regulatory compliance. Prior to joining First Healthcare Compliance, Ms. Vine was an attorney in private practice in the areas of litigation and employment law with the Jacobs Law Group, P.C., the Danneman Firm, LLC, and the Vigilante Law Firm, P.C. Previously, Ms. Vine held positions in the medical device industry with Hoffman La-Roche and Siemens. Ms. Vine received her Juris Doctorate from Widener University School of Law and her Bachelor of Science in Biomedical Engineering from Drexel University.

First Healthcare Compliance offers a comprehensive "turnkey" compliance program management solution to healthcare providers and others involved in managing healthcare compliance. The company also provides compliance management resources and CME online compliance courses. Find out more at www.1sthcc.com or 888.54.FIRST or shebavine@1sthcc.com.


Are you helping your customers conquer their revenue cycle challenges?
Healthcare is facing unprecedented change and mounting cost containment pressures. Alpha II partners with developers to integrate efficiency and accuracy into the revenue cycle of healthcare providers nationwide.
Make the right move towards more accurate coding, billing and reimbursement with Alpha II.
ALPHA II
www.alphaii.com