Extreme Caution: The HIPAA Dos and Don'ts When Responding to a Subpoena for Patient Medical Information

Stacey L. Zill, JD

Urgent message: When health-care providers or urgent care centers respond to subpoenas for patients' medical information, it is vital that they respond promptly, respond with exactly the information requested and nothing more, and protect patients' privacy and confidentiality.

Introduction

When producing documents in response to a subpoena demanding patient medical information, a health-care provider must know the *dos* and *don'ts* to avoid privacy and confidentiality violations, sanctions, and penalties. A subpoena is a court or administrative order requiring a provider to testify and/or produce documents at a specified time and location. This article offers guidance about what to do and what not to do after being served with a subpoena calling for the production of protected health information (PHI).[1]

The Dos and Don'ts

Don't ignore a valid subpoena; it will not go away if it is placed in a drawer or deposited in the round file. In fact, failure to respond can subject a provider to contempt sanctions. Even though the subpoena must be respected, *don't* produce PHI without protecting patient privacy and confidentiality, because the ramifications of not properly responding to a subpoena can be even more severe than those of ignoring the subpoena altogether. Indeed, the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations authorize heavy fines and potential criminal charges for the unlawful disclosure—whether oral, paper, or electronic—of PHI. Even inadvertent breaches can result in corrective action, hefty fines, administrative investigations, reputation damage, and loss of business. Therefore, it is critical that the responding provider know the *dos* for responding to a subpoena.

After being served with a subpoena, *do* confirm that it has been validly issued. For the subpoena to be valid and enforceable, the court or issuing agency must have jurisdiction over the provider. This generally means that a provider is located in the same state as the court or issuing agency. If there is no jurisdiction, a provider does not have to respond. In an abundance of caution, a provider should consult with counsel and/or serve objections in a timely manner. A provider can also file a motion to quash the subpoena, although this is an expensive option that may be overkill.

Once it has been determined that the subpoena requesting PHI was validly issued, the next step is to examine HIPAA privacy rules, which explain when a provider—or "covered entity"[2]—can disclose PHI. There are also state laws that govern the handling and production of patient medical records.[3] The general rule is that PHI must not be disclosed unless a regula-

Stacey L. Zill, JD, is a Los Angeles–based health-care litigator for Michelman & Robinson, LLC, focused on provider representation, including business and payment disputes, practice formation and corporate governance, compliance, breach of contracts, fiduciary duties, and unfair competition.

1. Discussion of a subpoena requesting mental health records is beyond the scope of this article.
2. A covered entity includes (1) a health plan, (2) a health-care clearinghouse, and (3) a health-care provider who transmits any health information in electronic form (title 45 of the Code of Federal Regulations, subtitle A, subchapter C, part 160, subpart A, section 160.103; available from http://www.ecfr.gov/cgi-bin/text-idx?SID=7675be34ca66e589d7a13c552a9d69fc&mc=true&node=se45.1.160_1103&rgn=div8).
3. If there is a conflict between state law and the Health Insurance Portability and Accountability Act, the law that provides the greater protection applies.

tory exception applies.[4] HIPAA contains exceptions for responding to subpoenas, but the rules differ according to the type of subpoena that is issued.

- **Subpoena signed by judge:** A provider should respond to a subpoena by providing the requested documents at the date and time set forth in the subpoena, issued by a judge or magistrate having jurisdiction over the provider, because HIPAA assumes that the issuing judge or magistrate considered patient privacy and confidentiality rights before signing the subpoena.[5] A provider, however, must be cautioned not to disclose more PHI than is ordered. For example, a provider should remove patient identifying information (e.g., patients' names, addresses, Social Security numbers, telephone numbers) if such details are not necessary to comply with the demands of the subpoena. A provider should not do an information dump and provide all of its documents relating to a patient if all that is requested is, for example, billing records. When documents are produced, it is helpful to affix a "confidential" stamp on each page.
- **Grand jury subpoena:** A provider may comply with a grand jury subpoena without violating HIPAA.[6] Grand jury proceedings are closed to the public, and because the information is kept confidential, HIPAA presumes that the patient's privacy interests are protected.
- **Administrative demand:** A provider may respond to an administrative subpoena if the administrative agent confirms (1) that the PHI sought is relevant and material to a legitimate law-enforcement inquiry, (2) that the request is specific and limited in scope to the extent reasonably practicable to accomplish the purpose for the demand, and (3) that de-identified information could not reasonably be used.[7]
- **Subpoena signed by clerk or attorney:** A provider may disclose PHI in response to a subpoena signed by a court clerk or attorney if one of the following conditions is satisfied:
  - *First*, the subpoena is accompanied by a written statement from the issuing party that (1) reasonable good faith efforts have been made to notify the patient in writing of the subpoena, (2) the notice included sufficient detail to permit the patient to object to the subpoena in court, and (3) the time for the patient to object to the subpoena has lapsed and either no objections were filed or the court has overruled the objections.[8]
  - *Second*, the subpoena is accompanied by a written statement from the issuing party that the parties to the proceeding have agreed to a qualified protective order that maintains the confidentiality of the information to be produced, or that such a protective order has been requested.[9] HIPAA defines a *qualified protective order* as an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested, and requires the return or the destruction of the PHI, including all copies made, at the end of the litigation or proceeding. Alternatively, a provider may seek its own protective order, but this is not likely to be a preferred option, given the expense.
  - *Third*, (1) the provider makes reasonable efforts to notify the patient (or the patient's lawyer) of the subpoena in writing, (2) the notice includes sufficient detail to permit the patient to object to the subpoena in court, and (3) the patient fails to quash or modify the subpoena and notify the provider of same.[10] By providing the patient with sufficient notice, a provider essentially shifts the burden to the patient to take appropriate steps to protect his or her own information. Alternatively, a provider may obtain a valid HIPAA authorization executed by the patient that complies with section 164.508 of title 45 of the Code of Federal Regulations. Although these may be the preferred options when the records of a few patients are being sought, such avenues may be unavailable or not practical where PHI of hundreds or thousands of patients is being sought.

If a provider cannot satisfy one of the foregoing, it may not disclose PHI but must instead wait for the court to order disclosure. Specifically, a provider should serve objections, which may be enough. In federal civil cases in which documents are requested, sending written objections based on HIPAA, and any other objections, to the party issuing

4. Title 45 of the Code of Federal Regulations, subtitle A, subchapter C, part 164, subpart E, section 164.502; available from http://www.ecfr.gov/cgi-bin/text-idx?SID=ba40f680a4d0ff4784e55a7167df9638&mc=true&node=se45.1.164_1502&rgn=div8

5. Title 45 of the Code of Federal Regulations, subtitle A, subchapter C, part 164, subpart E, section 164.512, paragraphs (e)(1)(i) and (f)(1); available from http://www.ecfr.gov/cgi-bin/text-idx?SID=ba40f680a4d0ff4784e55a7167df9638&mc=true&node=se45.1.164_1512&rgn=div8

6. Title 45 of the Code of Federal Regulations, subtitle A, subchapter C, part 164, subpart E, section 164.512, paragraph (f)(1)(ii)(B); available from http://www.ecfr.gov/cgi-bin/text-idx?SID=ba40f680a4d0ff4784e55a7167df9638&mc=true&node=se45.1.164_1512&rgn=div8

7. Title 45 of the Code of Federal Regulations, subtitle A, subchapter C, part 164, subpart E, section 164.512, paragraph (f)(1)(ii)(C); available from http://www.ecfr.gov/cgi-bin/text-idx?SID=ba40f680a4d0ff4784e55a7167df9638&mc=true&node=se45.1.164_1512&rgn=div8

8. Title 45 of the Code of Federal Regulations, subtitle A, subchapter C, part 164, subpart E, section 164.512, paragraphs (e)(1)(ii)–(iii); available from http://www.ecfr.gov/cgi-bin/text-idx?SID=ba40f680a4d0ff4784e55a7167df9638&mc=true&node=se45.1.164_1512&rgn=div8

9. Title 45 of the Code of Federal Regulations, subtitle A, subchapter C, part 164, subpart E, section 164.512, paragraphs (e)(1)(i), (iv), and (v); available from http://www.ecfr.gov/cgi-bin/text-idx?SID=ba40f680a4d0ff4784e55a7167df9638&mc=true&node=se45.1.164_1512&rgn=div8

10. Title 45 of the Code of Federal Regulations, subtitle A, subchapter C, part 164, subpart E, section 164.512, paragraph (e)(1)(vi); available from http://www.ecfr.gov/cgi-bin/text-idx?SID=ba40f680a4d0ff4784e55a7167df9638&mc=true&node=se45.1.164_1512&rgn=div8

the subpoena places the burden on the issuer to obtain a court order to compel production.[11]

A provider, however, should confirm whether the applicable state law has a similar provision. For example, some states have laws that will require a provider not only to object but also to file a motion to limit or quash the subpoena; simply objecting is not enough. If the subpoena calls for personal appearance as well as the production of documents, then as an alternative to serving objections or filing a motion to quash or limit the subpoena, a provider may simply show up at the date and time stated in the subpoena and, when asked to disclose PHI, object to disclosure on the basis of HIPAA. If a judge is present, a provider may then ask the judge whether disclosure is being ordered. In most cases, the judge will order the disclosure, and a provider may disclose such information pursuant to title 45 of the Code of Federal Regulations, section 164.512, paragraph (e)(1)(i),[12] and thus comply with the obligation to protect the patient's PHI.

Checklist for Responding to a Subpoena Requesting Protected Health Information

In light of the foregoing discussion, there are steps to be taken to comply with a subpoena while, at the same time, protecting patient privacy and confidentiality. A provider should do the following:

1. Confirm that the subpoena is validly issued
2. Identify the type of subpoena issued (e.g., grand jury, administrative demand) and the signatory to the subpoena (e.g., judge, administrative agency, attorney)
3. If the subpoena is signed by an attorney, contact the party issuing the subpoena to obtain satisfactory written assurances or a qualified protective order as already described
4. In an abundance of caution, and when the subpoena is requesting records relating to a limited number of patients, notify the patients whose records are being sought as already outlined and/or determine whether the patients will provide a valid HIPAA authorization that complies with title 45 of the Code of Federal Regulations, section 164.508[13]
5. If there are any questions about whether documents can be produced, serve objections on the party issuing the subpoena
6. Consider whether other laws in addition to HIPAA limit disclosures (e.g., limits on disclosures for mental health records and drug/alcohol treatment records, state laws relating to patient privacy, attorney–client privilege, peer review privilege)
7. Reach out to the party issuing the subpoena to discuss what exactly is being requested and a methodology by which a provider can comply with the subpoena while staying within the restrictions of HIPAA and applicable state laws (as, in most cases, that party is happy to reach an agreement)

"Don't ignore a valid subpoena; it will not go away if it is placed in a drawer or deposited in the round file. In fact, failure to respond can subject a provider to contempt sanctions."

If a provider is producing documents in response to the subpoena, *do* respect the exact terms of the subpoena. *Don't* produce more than required. *Don't* produce documents before the date and time identified in the subpoena, because the patient may need that time to take whatever action is necessary to attack or limit the subpoena. *Do* stamp documents as "confidential." Finally, *do* maintain a copy of the subpoena and a log of what was produced in response to it.[14]

Reimbursement of Costs Related to Compliance with a Subpoena

Federal law and most state laws allow a provider to recover its "reasonable costs" in responding to a subpoena, including, for example, postage, clerical charges, and fees for reproduction of documents. Before the production is made, a provider should contact the issuer of the subpoena to provide a cost estimate and secure an agreement that those costs will be paid before the production. States differ as to whether a provider still must produce the documents if an agreement is not reached or prepayment is not made. If the costs associated with compliance are significant, a provider may want to assert objections that are based on compliance being "burdensome and oppressive" and/or to seek judicial relief. This objection usually requires a showing of more than mere inconvenience.

Conclusion

When responding to a subpoena requesting PHI, a provider must *do* all that is required under HIPAA and applicable state laws to respect patient privacy and confidentiality. *Don't* take this responsibility lightly, because the repercussions may be severe. When in doubt, consult with counsel. ■

11. Title VI of the Federal Rules of Civil Procedure, rule 45, paragraph (c)(2)(B); available from https://www.federalrulesofcivilprocedure.org/frcp/title-vi-trials/rule-45-subpoena/
12. http://www.ecfr.gov/cgi-bin/text-idx?SID=ba40f680a4d0ff4784e55a7167df9638&mc=true&node=se45.1.164_1512&rgn=div8
13. http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=c77fd854b916b1fdeb3c76b1e0obebof6&ty=HTML&h=L&mc=true&r=SECTION&n=se45.1.164_1508
14. Title 45 of the Code of Federal Regulations, section 164.528; available from: http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=c77fd854b916b1fdeb3c76b1eobebof6&ty=HTML&h=L&mc=true&r=SECTION&n=se45.1.164_1528