Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

HIPAA and Subpoenas, Orders, and Administrative Demands

Insight — September 15, 2023

The HIPAA privacy rules (45 CFR § 164.501 *et seq*.) generally prohibit healthcare providers and their business associates from disclosing protected health information in response to subpoenas and other government demands unless certain conditions are satisfied. This outline summarizes HIPAA rules for responding to such demands. To the extent there is a more restrictive state or federal law that applies in a particular case, the more restrictive law will usually control.

SUBPOENA, COURT ORDER, WARRANT, OR ADMINISTRATIVE DEMAND. If a provider receives a subpoena, court order, or warrant that requires the disclosure of protected health information, the provider should do the following:

1. If the provider is named as a party in the action (e.g., the provider is the plaintiff or defendant), the provider should immediately notify its attorney. HIPAA contains an exception that generally allows a provider to disclose information in the course of litigation to which it is a party although the provider should take appropriate steps to disclose the minimum necessary. (*See* 45 CFR §§ 164.506 and 164.501, definition of "healthcare operations").

2. If the provider is not a party in the action, the provider should determine if the court or agency issuing the subpoena or order has jurisdiction over the provider. As a general rule, state courts or state agencies only have jurisdiction over entities located or operating within their state. State court or agency subpoenas, orders, or warrants issued across state lines are generally unenforceable; the subpoena must be issued by a court within the state in which the provider is located or in which it operates. The rules for federal court subpoenas or orders differ federal law generally allows a federal court or agency to issue a subpoena nationwide, although the location at which the witness must appear or produce records may be limited. (*See*, *e.g.*, Fed. R. Civ. Proc. 45(b)(2)). If the court or agency that issued the subpoena or order does not have jurisdiction over the provider, the provider is not obligated to respond to the subpoena or order. If there is any question about whether the court or agency has jurisdiction or whether the subpoena was properly served, the provider should contact its attorney or the entity issuing the subpoena to confirm its jurisdictional authority and/or explain that the entity will require a subpoena issued by a court or agency with appropriate jurisdiction before it will respond.

3. If the court or agency has jurisdiction over the provider, the provider's response will depend on the type of entity issuing the subpoena, order, warrant, or demand as described below. In essence, the HIPAA rules balance the need for disclosures in legal proceedings against patient privacy. To that end, the rules are designed to ensure that an independent judicial or administrative officer has authorized the disclosure, protections are in place to preserve confidentiality, or the person who is the subject of the subpoena has been notified and given the chance to object to the disclosure. (*See* 45 CFR § 164.512(e)).

   Significantly, if the court or agency had jurisdiction to issue the subpoena, the provider may not simply ignore the subpoena or demand without risking contempt sanctions even though HIPAA limits disclosures; instead, it should take one of the foregoing steps to respond appropriately. State and federal rules generally allow a witness or other person who receives a subpoena to recover certain coping costs or witness fees. The costs and fees are usually limited and are listed in court rules or statutes. If the response would create an undue burden on the provider, the provider may contact the party issuing the subpoena to explain the burden and negotiate a resolution and/or file a formal objection with the court. The provider should discuss such objections with its own attorney.

   a. **Court Order, Warrant, or Subpoena Signed by a Judge or Magistrate.** If the order, warrant, subpoena, or summons is signed by a judicial officer (i.e., signed by a judge or magistrate) or an administrative tribunal, the provider should strictly comply with and disclose the information expressly authorized by the order, warrant, subpoena, or demand. (45 CFR § 164.512(e)(1)(i) and (f)(1)(ii)). Failure to do so may result in contempt sanctions, including fines or penalties against the provider. The provider should not disclose more than the information required by the order and should limit the disclosure to the manner specified in the order.

   b. **Grand Jury Subpoena.** If the subpoena is issued in a grand jury proceeding, the provider should strictly comply with its terms. Grand jury proceedings are confidential, so HIPAA does not require additional protections. (45 CFR § 164.512(f)(1)(ii)). The subpoena itself will generally state if it is issued by a grand jury.

   c. **Subpoena Signed by Court Clerk, Lawyer, Prosecutor, or Other Non-Judicial Officer.** If the subpoena or other lawful process is signed by a person other than a judge, magistrate, or administrative tribunal (e.g., it is signed by a lawyer, prosecutor, court clerk, etc.), HIPAA wants to make sure the patient has been given notice of the subpoena, has had the chance to object, and/or that an appropriate protective order is in place. To that end, the provider may

not disclose protected health information before it has satisfied one of the following alternatives in 45 CFR 164.512(e)(1):

i. The provider should contact the patient who is the subject of the requested protected health information either orally or by letter, explain that the provider has received a subpoena requiring disclosure of the patient's information, and notify the patient that the provider is required to respond unless the patient quashes the subpoena and notifies the provider before the deadline for responding to the subpoena. (45 CFR § 164.512(e)(1)(vi)). Once the provider sends such notice, the burden is on the patient to quash the subpoena if he or she wants to protect the information. A sample letter can be found here. This is often the easiest and most cost-effective way for a healthcare provider to handle these matters and removes the provider from the middle of the dispute.

ii. Alternatively, the provider may obtain satisfactory written assurances from the entity issuing the subpoena that either: (a) the entity made a good faith attempt to give the patient written notice of the subpoena, the notice included sufficient information to permit the patient to object to the subpoena, and the time for raising objections has passed or the court ruled against the patient's objections; or (b) the parties have agreed on a protective order or the entity seeking the information has filed for a protective order. (45 CFR § 164.512(e)(1)(iii)-(iv)). This alternative can be time consuming and less certain than option (i), above.

iii. Alternatively, the provider may obtain a valid HIPAA authorization to disclose the information executed by the patient. To be valid, the authorization must contain the elements and statements required by 45 CFR § 164.508. If the subpoena is issued by the patient's lawyer, the provider may contact the patient and confirm that the patient authorizes the disclosure to the lawyer, in which case the provider can likely rely on the patient's consent to make the disclosure per 45 CFR §§ 164.510(b)(1) or 164.524.

iv. Alternatively, the provider may appear at the time or place indicated in the subpoena and object based on HIPAA, but this will likely require additional time and expense for the provider and, in all likelihood, the court will require disclosure anyway. It is usually easier to go with one of the other alternatives.

d. **Administrative Subpoena, Summons, or Investigative Demand.** If the provider receives an administrative subpoena, summons, investigative demand, or similar process authorized by law, the provider may comply with the request if the issuing entity confirms: (a) the information sought is relevant and material to a legitimate law enforcement inquiry; (b) the request is specific and limited to the extent reasonably necessary for the purpose of the request; and (c) de identified information could not reasonably be used. (45 CFR § 164.512(f)(1)(ii)).

4. In rare but appropriate cases, the provider may petition the court for a protective order or move to quash a subpoena, order, or warrant. (45 CFR § 164.512(e)). The provider should contact the provider's attorney immediately if they believe the provider should seek a protective order or quash the subpoena. This will require additional time, cost, and inconvenience for the provider, so it is usually more cost-effective to respond through one of the alternatives identified above.

5. In all cases where disclosure is required, the provider must ensure that it complies with the strict terms of the subpoena, including the scope of the information disclosed and the timing of disclosure. If the subpoena, order, or warrant only requires disclosure of written items, the provider should not disclose the information orally. If the subpoena, warrant, or order requires disclosure at a specific time, the provider should not disclose the information before the deadline or outside the formal process specified in the subpoena or order (e.g., through phone calls or informal discussions with the party, lawyer, or prosecutor issuing the subpoena) without the patient's consent because doing so may deprive the patient of the opportunity to object to disclosure.

6. The provider should maintain a copy of the subpoena, order, or warrant, and document the facts of the disclosure in the Provider's disclosure log required by 45 CFR § 164.528.

WORKERS COMPENSATION. HIPAA contains a separate exception that allows a provider to disclose information as authorized by and to the extent necessary to comply with laws relating to workers compensation. (45 CFR § 164.512(1)). The provider should ensure they are familiar with the limits of their state's workers compensation laws and limit the disclosure to the extent required by those laws.

PUBLIC HEALTH ACTIVITIES. Under HIPAA, a provider may disclose protected health information to an entity authorized by law to conduct certain public health activities, e.g., to report certain communicable diseases. The provider should ensure the disclosures satisfy the requirements in 45 CFR § 164.512(b).

HEALTH OVERSIGHT ACTIVITIES. HIPAA also permits a provider to disclose protected health information to a health oversight agency (e.g., state licensing boards, CMS, OIG, etc.) for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight. The provider must ensure that it complies with the circumstances and limitations in 45 CFR § 164.512(d).

LAW ENFORCEMENT. HIPAA contains a whole series of exceptions related to disclosures to the police or other law enforcement agencies. (45 CFR § 164.512(f)). For more information about the appropriate response to law enforcement requests, see our Client Alert at https://www.hollandhart.com/police-providers-patients-and-hipaa.

NONCOMPLIANT REQUESTS. If a provider receives a request for protected health information that does not fit within a HIPAA exception (including the exceptions identified above), it may want to respond by sending an appropriate letter explaining its obligations under HIPAA. A sample letter can be found here.

OTHER LIMITATIONS. When evaluating the foregoing disclosures, providers should consider whether other laws in addition to HIPAA limit disclosures, e.g., limits on disclosures for substances use disorder records protected by 42 CFR part 2 or similar state laws; attorney-client privilege; peer review privilege; etc. Remember: to the extent a state law is more restrictive than HIPAA, providers are generally required to comply with the more restrictive law. Providers should work with their attorneys to evaluate such situations.