



*Rich Glass is chief compliance officer for Infinisource, Inc. He is a licensed attorney and brings more than 15 years of legal expertise, specializing in benefits, human resources and related regulatory compliance. He has testified before the Internal Revenue Service and has provided comments on regulations issued by several governmental authorities. He is a member of Thompson Publishing Group's Health Plan Advisory Panel. He is a frequent speaker and author on various benefits, employment law and compliance issues.*

# You Received a Subpoena for PHI, Now What?

*By Rich Glass, J.D.*

Nothing can cause a benefits or human resources professional more heartburn than to look through the daily mail and find a subpoena for records. But before you spend quality time with a copier, you should take several precautions, especially if the request pertains to one or more employees' health information.

Subpoenas may be issued in various circumstances. Many local, state and federal governmental agencies, including law enforcement, have the power of subpoena to gain access to records that are relevant to the laws and regulations they administer. Subpoenas may be issued by a court or an attorney. They can request testimony (by deposition or in some other judicial or administrative proceeding), documents (in a *subpoena duces tecum*) or both. The recipient of a subpoena need not be a party to the lawsuit. The information request also may take a form other than a subpoena, like a discovery request or administrative order.

When you receive a subpoena that might relate to HIPAA-protected information, review it closely before complying. Employers and other plan sponsors should consider the following five-step process.

## 1) Clarify the Requirements

Look at the document to determine the time and place that records are expected to be delivered. If these expectations are unrealistic, you should request more time. The party issuing the subpoena will often be willing to accommodate reasonable extension requests.

To whom is the subpoena addressed? This is an important consideration because HIPAA's use and disclosure restrictions apply only to covered entities. As you may recall, the covered entity is usually not the employer/plan sponsor, but the underlying health plan itself (see ¶131 of the *Guide*).

If the subpoena is requesting the employer's documents, look for language that determines the scope of the request. A request for

documents in the care, control, possession or custody of the employer arguably includes a request for documents from the plan, the covered entity. On the other hand, if the subpoena only seeks the documents of the employer, an employer should clarify that certain documents may be obtained from the HIPAA-covered entity (that is, the plan).

## 2) Determine Whether Any Requested Information Is PHI

Recall that not all health information is protected health information (PHI) under HIPAA. PHI is individually identifiable health information that is maintained or transmitted by a covered entity and relates to the past, present or future health or condition of an individual, the provision of care or the payment for such care (see ¶201). Therefore, PHI does not include employment-related records like workplace drug testing results, reasonable accommodation documents under the Americans With Disabilities Act and certifications under the Family and Medical Leave Act.

Summary health information is not PHI because it does not include individual identifiers. Health plan enrollment data received by an employer are typically not viewed as PHI until they are sent to the covered entity or its business associate (such as a self-funded plan's claims administrator). (These exceptions are detailed in ¶321.)

If the plan is compelled to provide PHI, it must provide the minimum amount necessary to comply with the subpoena (see ¶311).

## 3) Ensure That Disclosure Is Permitted

In this step, there are two different paths, one if the subpoena recipient is a party to the litigation or other proceeding and another if the subpoena recipient is not:

- *Recipient is a party.* The path in this situation is fairly straightforward. PHI disclosure is permitted without the

**See Subpoena, p. 5**

## Subpoena (continued from page 4)

individual's authorization because this is viewed as the covered entity's health care operations (see ¶215).

- *Recipient is not a party.* Scrutinize the subpoena and any other documents that were included to see if the subpoena was issued under the order of a court or administrative tribunal. If so, you may proceed with responding to the request.

Things get more complicated when a nonparty receives a subpoena without a court order. Such a subpoena must also include a written statement providing "satisfactory assurances" that the requesting party is complying with HIPAA. This means that it has made reasonable efforts to notify the individual whose PHI is at issue by sending a written notice to the last known address. The notice must tell the individual about the litigation or proceeding so that he or she has time to object to the request. The time to object must have expired, and any objections must have been resolved.

If the requesting party did not notify the individual, it must demonstrate that it made reasonable efforts to obtain a qualified protective order. This type of order limits the requesting party's use of the PHI to the litigation and, when litigation ends, calls for the PHI's return or destruction.

Thus, unless a subpoena to a nonparty includes this written, satisfactory assurances statement, HIPAA does not permit disclosure. (See ¶342.)

## Genetic Data (continued from page 2)

### Enforcement

GINA Title I imposes penalties of up to \$100 per day per affected participant or beneficiary, up to an overall limit of \$500,000 or 10 percent of the plan sponsor's total annual health plan expenditures provided the violations were due to reasonable cause, not willful neglect. The bill was amended shortly before its enactment to address concerns that it could expose plan sponsors to the full panoply of employment-law liability along with the ERISA and PHSA penalties (see May 2008 newsletter).

As under HIPAA's privacy provisions, plans can avoid penalties if they did not know, and by exercising "reasonable diligence" could not have known, of the violation — or if they correct it within 30 days of finding out about it (see ¶620). However, a plan sponsor or insurer that fails to correct a violation before being notified

## 4) Document the Request and What Was Provided

One of the overlooked HIPAA requirements is that covered entities must account for all disclosures. One exception to the accounting requirement is when the disclosure is a routine one that involved treatment, payment or health care operations. Another exception is when the covered entity receives authorization from the individual. Therefore, when the subpoena is addressed to a party of the litigation, it is a routine disclosure. These disclosures are considered health care operations, and no accounting is necessary.

---

### Things get more complicated when a nonparty receives a subpoena without a court order.

---

Otherwise, the covered entity must account for all unauthorized disclosures and provide the accounting to the individual upon request (see ¶435).

## 5) Seek Help When Needed

When in doubt, ask for help from competent legal counsel that understands HIPAA and any relevant state laws that may be more restrictive than HIPAA. Of course, another option is to alert the individual to the subpoena and simply obtain written authorization (see ¶410). Then there is little danger of violating HIPAA or state law.

In summary, not all subpoenas are created equal. A subpoena is not a magic word or phrase like "open sesame" that automatically justifies disclosing PHI. ⬆

by the appropriate agency will be fined at least \$2,500 per participant — \$15,000 if the violation is "more than *de minimis*."

### Employer Provisions

The employer provisions of Title II are modeled on employment discrimination laws like the Americans With Disabilities Act. Of note from a privacy standpoint, Title II generally prohibits employers from collecting employees' genetic information, and requires any such data an employer does possess to be kept in separate, confidential files.

However, genetic data may be collected on a limited basis for employee wellness programs (see ¶215), and an employer may require an employee's family medical history as needed to comply with the Family and Medical Leave Act (see ¶730). ⬆

New! Try HR 2008: Answers to Your Top 25 Questions for 30 days. [www.thompson.com/answ](http://www.thompson.com/answ)