



HIPAA – RESPONDING TO LEGAL PROCESS

The Health Insurance Portability and Accountability Act (HIPAA) and its Privacy regulations have exacerbated the sometimes difficult relationship between health care providers and attorneys seeking access to confidential patient information to further the legal rights and interests of persons they represent. At times, however, the Privacy Rule has little to do with the angst that a medical provider and an attorney may experience over a medical record request. In the end, the relationship between an attorney and a medical provider must be grounded not only in an enhanced knowledge of the law but also in fundamental respect for each party's legitimate professional needs and interests.

Attorneys generally seek medical record information from health care providers through use of subpoenas, subpoenas duces tecum, warrants, and court orders. There are differences among these forms of legal process. And there is no uniformity in format and language for them.

Health care providers must carefully review all forms of legal process to assure compliance with HIPAA's requirements and other risk management considerations. A provider must respond to legal process by either releasing the requested information or, if problems are identified, by working things out with the requesting attorney or by taking appropriate legal action to quash legal process. Failure to respond subjects the health care provider to court sanctions.

FORMS OF LEGAL PROCESS

Subpoena: Compels a person to appear and give testimony either for deposition or in a court proceeding. Subpoenas are available from the clerk of court without showing cause. A court does not review the subpoena before it issues. Nonetheless, a subpoena is supported by the authority of the courts. "Subpoena" means "under penalty." Failure to timely respond subjects the recipient to court sanctions.

Subpoena duces tecum: "Duces tecum" loosely means: bring things with you. A subpoena duces tecum compels the recipient to attend and to also bring requested documents. A subpoena duces tecum is not the same as a court order but it is supported by court authority. Failure to timely respond will subject the recipient to court sanctions.

County attorney's subpoena: County attorney subpoenas issued in criminal cases may be the equivalent of an order of a court. Language on the face of the subpoena will state as such. Absent such language, a health care provider should treat a county attorney's subpoena the same as an ordinary subpoena.

Federal subpoena: Subpoenas issued through the federal courts generally are treated like state court orders.

Search warrant: This infrequently used legal process generally is employed by government investigators and law enforcement to conduct a search and seizure of files and space consistent with the directive of the warrant itself. Warrants are issued by a court based upon a finding of probable cause. A search warrant is the equivalent of a court order.

Court order: Court orders for medical records are issued after the court has heard from the parties and determined that the requested medical record information is lawfully subject to production. The face of a court order will include a caption identifying the court and will include the signature of the judge issuing the order.

Administrative subpoenas or warrants: These subpoenas and warrants are issued under the authority of a federal or state agency of government with investigative and enforcement authority. Health care providers risk administrative and court sanctions for failing to timely respond either by releasing the requested medical record information or by moving to challenge the subpoena or warrant as appropriate either before the agency or in the courts.

Q & A: RELEASE OF PHI PURSUANT TO LEGAL PROCESS UNDER HIPAA

Does HIPAA's Privacy Rule permit a covered entity to release PHI to attorneys preparing for litigation?

Yes, but only if HIPAA's conditions for use or disclosure are met. HIPAA's governing standard says that a covered entity may not use or disclose PHI except as permitted or required by the Privacy Rule. Rule 164.502(a).

Under the Privacy Rule, may a covered entity that is a party in a legal proceeding use or disclose PHI to prepare for litigation either as a plaintiff or as a defendant?

Yes. The OCR has issued a specific advisory on this point. A covered entity may use or disclose PHI for purposes of litigation within the scope of its health care operations so long as the litigation is related to the covered entity's covered functions. Rules 164.501, 164.506(a). The covered entity must make reasonable efforts to limit such uses and disclosures to the minimum necessary to accomplish the intended purpose. Attorneys receiving such information either as workforce members or business associates of the covered entity also must make reasonable efforts to limit the PHI disclosed to that minimally necessary for purposes of the disclosure. FAQ Answer ID 705. Similarly, attorneys receiving PHI from their covered entity clients under a business associate's agreement must be aware of additional responsibilities they may have relative to further use and disclosure of that PHI. FAQ Answer ID 709. Finally, a covered entity may release PHI to its professional liability carrier for purposes of obtaining benefits and maintaining coverage. FAQ Answer ID 274.

Under the Privacy Rule, may a covered entity release PHI to an attorney seeking access to medical record information for litigation purposes where the covered entity is not a party to that litigation or proceeding?

Yes, but, again, only consistent with the requirements of the Privacy Rule. The Privacy Rule provides three primary routes under which covered entities may release PHI to attorneys for purposes of litigation or administrative proceedings in which the covered entity is not a party: 1) a HIPAA-valid authorization executed by the individual subject of the requested PHI or the individual's personal representative, Rules 164.508(a), 164.508(b)(1)(i); 2) an order of a court or administrative tribunal, Rule 164.512(e)(1)(i); or (3) other legal processes supported by satisfactory assurances required by Rule 164.512(e)(1)(ii).

Usually the easiest and most direct route for attorneys is to request PHI pursuant to a HIPAA-valid patient authorization. A subpoena or subpoena duces tecum issued with a valid authorization works.

An order from a court or administrative tribunal compelling the release of medical record information generally is a last resort. A covered entity may release PHI based on such order but also must assure that the disclosure is limited to PHI expressly authorized by the order. Rule 164.512(e)(1)(i); FAQ Answer ID 703.

Absent the individual's authorization or an order of a court or administrative tribunal, a covered entity can release PHI only under legal processes accompanied by "satisfactory assurances" set forth in the Privacy Rule. Rule 164.512(e)(1)(iii); FAQ Answer ID 711.

What makes an authorization "valid" under the HIPAA Privacy Rule?

A valid authorization must 1) be written in plain language; 2) include certain "core elements"; and 3) contain certain "statements." Core elements include a description of the information to be disclosed; name of person authorized to make the disclosure; name of person to receive the disclosure; description of each purpose of the disclosure; expiration date or event; signature of the individual or individual's personal representative; and date. Statements must be adequate to put the individual on notice of the individual's right to revoke; the ability or inability of the covered entity to condition treatment on the individual's execution of an authorization; and consequences associated with redisclosure by the recipient. Rule 164.508(c)(1-3); FAQ Answer IDs 706, 711.

An authorization is *defective* if the expiration date has passed or the specified expiration event has occurred; the form has not been completed as required; the authorization has been revoked; a material statement in the authorization is false; or the authorization otherwise violates the requirements of the Privacy Rule. Rule 164.508(b)(2).

Can a covered entity health care provider require an attorney to use its authorization form?

The Privacy Rule requires a covered entity to assure that an individual's authorization for release of the individual's PHI is valid under HIPAA. Rather than evaluate each authorization provided to it, the health care covered entity may elect to require use of its own form. The provider's response is fair and appropriate under HIPAA.

The Iowa State Bar Association's (ISBA) patient authorization form (July 2004) is HIPAA compliant. Hospitals and physicians generally are aware of this and readily accept the ISBA form in lieu of their own. That form is accessible at www.iowabar.org

Is an attorney representing a person in litigation a "personal representative" with the same right of access as the individual to the individual's PHI under the Privacy Rule?

No. Under the Privacy Rule, a *personal representative* is a person with authority under state law to act on the individual's behalf on matters related to *health care*. FAQ Answer ID 224. An attorney representing a client in litigation is *not* that client's personal representative. An attorney-in-fact named as an agent in the individual's durable power for health care is a personal representative under HIPAA. The distinction is important.

If an attorney has a validly executed, HIPAA-compliant patient authorization for release of PHI but the patient has not specifically authorized release of mental health, substance abuse, and/or HIV/AIDS information, what is the best course to follow?

Health care providers bear special risk under federal and state laws for unauthorized release of mental health, substance abuse and HIV/AIDS information. Health care providers need either a patient authorization specifically permitting the release of this information *or* a court order court issued consistent with applicable federal or state law. Further information on the relationship between HIPAA and federal laws on substance abuse and HIV/AIDS is available on the OCR website, www.hhs.gov/ocr/hipaa/.

What is needed to assure a HIPAA-compliant release of PHI pursuant to a subpoena?

In order to comply with the Privacy Rule, a covered entity may disclose PHI pursuant to a subpoena supported either 1) by a HIPAA-valid patient authorization, or 2) by an order of a court or administrative tribunal; or 3) by "satisfactory assurances."

"Satisfactory assurances" required by the Privacy Rule can take on either of two forms. The first and most common form of satisfactory assurances requires a written statement along with documentation demonstrating to the covered entity a) that the party has made a good faith attempt to provide written notice to the individual subject of the PHI; b) that the notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection; and c) that time for the individual to raise objections has elapsed and either the individual failed to file objections or the objections have been resolved by the court or administrative tribunal. Rule 164.512(e)(1)(ii)(A); FAQ Answer ID 711. Notice to the individual is adequate if given to the individual's attorney of record. FAQ Answer ID 707.

The second form of satisfactory assurance demonstrates to the covered entity that the party requesting the PHI has made reasonable efforts to secure either a qualified protective order of a court or administrative tribunal or a stipulation of the parties that prohibits the parties from using or disclosing the PHI for any other purpose and requires the return of the PHI at the end of the litigation or proceeding. Rule 164.512(e)(1)(ii)(B); FAQ, Answer ID 711.

Can a covered entity release PHI pursuant to a HIPAA-valid authorization if the requested PHI was created after the authorization was signed by the individual?

Yes. This was an issue of confusion in the early days of Privacy Rule implementation. Unless otherwise expressly limited by the authorization, a covered entity may disclose PHI identified on the authorization regardless of when the information was created. Covered entities must assure that the authorization encompasses the category of PHI later created and that the authorization has not expired or been revoked. FAQ Answer ID 477.

Does the HIPAA Privacy Rule address fees that may be charged for medical records?

Yes, to a limited extent. The Privacy Rule addresses fees a covered entity may charge the *individual* (or personal representative of the individual, *see discussion above*).

If the individual requests a copy of the individual's PHI or agrees to a summary or explanation of such PHI, the covered entity may impose a reasonable, cost-based fee reflecting *only* the cost of 1) copying, including the cost of supplies for and labor of copying; 2) postage, if the individual requests that the copy or the summary be mailed; and 3) preparing an explanation or summary of the PHI if agreed to by the individual. The fee charged the individual may *not* include costs associated with searching for and retrieving the requested PHI. Rule 164.524(c)(4); FAQ Answer ID 353.

The Privacy Rule does not regulate fees for medical records when a person other than the individual or the individual's personal representative requests copies. As a result, many medical practices have adopted two medical record fee schedules. "Reasonableness" governs fees in non-HIPAA situations except in worker compensation cases where fees for production of medical records are set by rule. Iowa Administrative Code r. 876-8.9.