PROPER HANDLING OF MEDICAL RECORDS IN PERSONAL INJURY CASES

Wendell W. Walsh
May Oberfell Lorber
October 20, 2016

A. SUBSTANCE

1. PROTECTING SENSITIVE MEDICAL RECORDS

A personal injury plaintiff impliedly waives the physician-patient privilege as to those conditions causally and historically related to the claimed injuries. See *Collins v. Bair*, 268 N.E.2d 95 (Ind. 1971). It is perfectly understandable that a plaintiff may be uncomfortable with the review of private medical records concerning conditions of an intimate nature. Indiana law takes such concerns into account.

Who decides what medical records are discoverable? The plaintiff-patient? Her lawyer? Her doctor? A clerk at her doctor's office? The Court?

Who has the burden of demonstrating that a medical record is not discoverable?

Under what circumstances is the Court's time properly taken up with *in camera* review of medical records?

We do well to carefully read *Canfield v. Sandock*, 563 N.E.2d 526 (Ind. 1990); see also, *Andreatta v. Hunley*, 714 N.E.2d 1154 (Ind.Ct.App. 1999). The Supreme Court in *Canfield* teaches us that only when the medical records pertain to conditions of the most intimate nature, the trial court may be asked to review the records *in camera* by the plaintiff, who has the burden of demonstrating that the records are not discoverable.

> Once a privilege has been invoked, the burden is on the party claiming it to prove his entitlement to its protection.

Id., at 531.

> (C)ourts disfavor blanket claims of privilege such as that asserted [in this case]. *Petersen v. U.S. Reduction Co.*, 547 N.E.2d 860, 862 (Ind.Ct.App.1989). The party seeking to assert a privilege has the burden to allege and prove the applicability of the privilege "as to each question asked or document sought." *Owens v. Best Beers of Bloomington, Inc.*, 648 N.E.2d 699, 702 (Ind.Ct.App.1995) (citing *In re Walsh*, 623 F.2d 489, 493 (7th Cir.), cert. denied, 449 U.S. 994, 101 S.Ct. 531, 66 L.Ed.2d 291 (1980)). Claims of privilege "must be made and sustained on a question-by-question or document-by-document basis." *Petersen*, 547 N.E.2d.

Hayworth v. Schilli Leasing, Inc., 669 N.E.2d 165, 169 (Ind. 1996). Further:

> (T)he bare assertion of a claim of privilege will not suffice to block discovery of the information sought by the discovery request. Rather, the trial court must review the contested materials and determine whether the claim of privilege is justified or mistaken and whether production of the requested documents should be barred or compelled.

Canfield, at 531.

The Supreme Court in *Canfield* goes on to discuss the infrequent need for *in camera* review.

> Such a procedure should remain rare. **The expectation of all parties should be that . . . requested documents are either relevant and discoverable or irrelevant but innocuous such that no harm will result from disclosure, that discovery will proceed without the court's participation, and that invocation of the privilege will be preserved to protect from discovery information about only those conditions of the most intimate nature.** (Emphasis supplied).

Canfield, at 531.

There it is. Our Supreme Court has provided succinct guidance to trial courts and trial lawyers on this topic. Lawyers continue to review medical records which, although technically irrelevant, are *innocuous such that no harm will result from disclosure.* This happens all the time. Private review by a trial court is reserved for those records reflecting *only those conditions of the most intimate nature.* "*(I)n camera* inspections . . . should be a rare procedure in discovery disputes." *Richey v. Chappell*, 594 N.E.2d 443 (Ind. 1992).

2. TRANSMITTING MEDICAL RECORDS

What if counsel for a health care provider responds to a RFP by sending a CD with a patient's medical record, and the CD somehow goes to the wrong person? If you think this is unlikely, you probably have not used the U.S. Mail recently.

HHS regs provide that if the protected health information (PHI) is not secure (i.e. encrypted) counsel (as a business associate of the health care provider) must report the breach. That's a phone call no one ever wants to make. The patient's privacy may be compromised and the client may face an expensive, time consuming notice procedure under HIPAA.

> A covered entity shall, following discovery of a breach of **unsecured protected health information**, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

45 C.F.R. §164.404(a)(1).

> A business associate shall, following discovery of a breach of **unsecured protected health information**, notify the covered entity of such breach.

45 C.F.R. §164.410(a)(1).

According to 45 C.F.R. §164.402(1)(iii) and (2):

> "[The term] Breach excludes: . . . (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
>
> * * *
>
> **Unsecured protected health information** means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

TRANSLATION: By using the specified methodology (encryption) the PHI is not "unsecured" (sorry for the double negative, but we are talking about Federal regs here). Since the PHI is not "unsecured" there would be no breach, and therefore no duty to notify.

The patient is entitled to notice of a request for production. *See* 45 C.F.R. §164.510. So, when the request comes from a co-defendant, check to be sure a copy of the request was sent to the patient's attorney.

Then, encrypt the medical records and send the password under separate cover. In this way, the PHI is "secured", as defined by HHS regulations. This procedure addresses the rare case in which PHI is lost or received by the wrong recipient. In such a case, the unintended recipient cannot access the information and there is no breach.

B. TIPS

1. PROTECTING SENSITIVE MEDICAL RECORDS

Counsel for the plaintiff should thoroughly discuss with the client whether there have been "conditions of an intimate nature." Obtain the records and be prepared to submit them for *in camera* review, if they are requested.

Counsel for the defendant should submit a memorandum setting out the medical issues to guide the court during *in camera* review.

2. TRANSMITTING MEDICAL RECORDS

Make sure the patient's attorney is on notice of a request for records. Allow time for the patient to raise objection.

Send only encrypted records, with the password being sent under separate cover.

C. TRICKS

Sorry, there are no tricks. Nor should there be. There's a common sense, "golden rule" aspect to this: Treat the medical records in the same dignified fashion as you would want the records of a person close to you.