Release of Information: When to Call a Healthcare Compliance Attorney

By Barry S. Herrin, JD, CHPS, FACHE, FAHIMA

The HIPAA-HITECH modifications to the Privacy and Security Rules have made the management of the release of information function even more complex for providers. Add in state law and other protections, and it can be difficult for health information management (HIM) professionals to know just when it is legal to release protected health information (PHI) to patients and other providers.

Meanwhile, the consumer engagement, interoperability, and health information exchange initiatives growing in healthcare are calling on healthcare professionals to be more open with the exchange of PHI and improve patient/caregiver access to health records. This loosening of restrictions can create an environment where HIM professionals may improperly release medical records—relying on peer advice, industry benchmarks, or just the "legend" and "lore" in the HIM industry to guide their decisions instead of following actual legal requirements.

A lot can go wrong when it comes to release of information (ROI), and sometimes the best thing to do is consult a healthcare attorney for advice. Many HIM professionals are over-stressed and under-resourced, which adds to the burden of making the right legal call on gray-area ROI requests. The following examines some of the common ROI misunderstandings and pitfalls of HIM professionals, and offers insights from an HIM-credentialed attorney with over 25 years of experience.

Requests Involving Minor Patients

Most states allow minor patients to consent to medical treatment—and, accordingly, to control the use and disclosure of medical record information of such treatment—when seeking services for prevention, diagnosis, and treatment of venereal diseases, pregnancy or termination of pregnancy, contraception, abuse of controlled substances or alcohol, or mental health services on an outpatient basis. Minors also may consent to treatment and release of information if they have been emancipated by marriage or when they have been emancipated by court decree or other statutory exceptions (i.e., enlistment in the US Armed Forces is a common emancipating condition in many states). In addition, most states allow minor patients to consent to any treatment for themselves in emergency circumstances. However, unless a minor is a Medicaid beneficiary or is requesting services at the emergency department, providers are under no general legal obligation to treat an unaccompanied minor, emancipated or not, even if the minor is an established patient.

One reason to deny minors access to care is because healthcare providers cannot meaningfully manage the disclosure of the minor's record. If the minor self-refers for a treatment episode, the parent or guardian generally has no right to know anything about the care. If the minor presents the parent's health insurance card, the provider is probably obligated to tell the minor patient that their parent will find out about the treatment and offer the minor the ability to pay full charges out-of-pocket so as to invoke HIPAA's privacy embargo on release of information (45 CFR 164.522(a)(1)(vi)).

Other problems occur after a minor reaches the age of majority. Once a minor becomes an adult, his or her parents lose all control over access to any of his or her healthcare records, unless the person continues to be covered on the parents' healthcare insurance. Even in this circumstance, the provider is probably under an obligation to explain to the "new adult" that even though he or she controls the medical record of care, his or her parents will still find out if the insurance company gets a claim.

This is yet another opportunity to offer the patient the chance to pay full charges out of pocket to avoid an unwanted privacy disclosure. In addition, if the "new adult" never signed anything while receiving care as a minor, the provider has no way to authenticate the identity of the patient when he or she requests records the very first time. In states that prohibit the copying of government identification cards this is made especially difficult, as the provider cannot request that the patient e-mail or fax a

copy of a driver's license. Therefore, the provider will be challenged to verify the signature of the patient unless he or she first appears in person—which is cumbersome at best, perhaps impossible at worst if the patient has relocated to college and needs the record for enrollment, student insurance, sports physicals, etc. And because they are an adult, Mom or Dad can't just come around and pick up a copy for the young adult like they did before.

The 'Myth of Redisclosure' and Records Received from Third Parties

For years, healthcare attorneys have encountered stubborn resistance to the concept that "all" of a patient's medical record does indeed mean "all" of that record, particularly in the context of records provided in the course of litigation. Usually the discussion revolves around a provider refusing to produce a portion of its medical record that was received from another source, such as another physician's office, another hospital, or even from the patient in an unsolicited production. So let's set the record straight.

First, federal law does not prohibit the redisclosure of these records, except in two very limited circumstances. One circumstance involves records created by drug and alcohol treatment programs that receive federal assistance, as explained in 42 C.F.R. Part 2. Absent the specific authorization of the patient, providers maintaining or receiving records of this type of treatment may not disclose it to anyone else. In fact, the sending organization is supposed to mark each and every page of such records with a noticeable disclaimer (which is set forth in the regulations) reminding the recipient of the prohibition against redisclosure. The second circumstance is not universal but applies to many state Medicaid programs. In these states, if a Medicaid beneficiary claims damages in a tort suit and if the medical care necessitated by the compensable injury was covered by Medicaid, then Medicaid has a right of subrogation against any judgment the beneficiary receives in the tort action. In order to prove the amount of the subrogation right, providers may be required to submit records. These records, in this limited circumstance, may not be redisclosed, and a disclaimer must be placed on each and every page of these records as well. Other than these two circumstances, there is no legal prohibition on the redisclosure of records received from other providers that are part of your official patient record of care.

Second, many HIM professionals believe that they cannot certify the truth of records not created in their own practices or facilities. This is bunk. The fact of the matter is that unless the records manager is a sole practitioner and does all of his or her own records maintenance and handling, no HIM professional has any idea whether the contents of the practice's or facility's own records are objectively true—that is, you don't know whether the blood pressure was recorded accurately or whether the X-ray really shows cancer. You presume everything in the record is true, but you have no actual knowledge whether it is or not. The certificate of the records manager, therefore, can only relate to the contents of the copy he or she is being asked to produce, and whether the copy contains the same information as the original. In other words, if the stack of paper to be copied looks just like the copy, the records manager has provided a true and accurate copy.

Unsolicited Health Information and the New World of Interoperability

With the push towards interoperability and the free exchange of information between patients and providers, problems continue to arise concerning how to handle unsolicited health information. This can be information that is "volunteered" by patients or by other healthcare providers, either at the time the patient arrives for treatment or thereafter, and in some cases even after the patient has been discharged. Traditionally, many providers felt compelled to accept such information, but were uncertain where to store it and so filed the information under the "miscellaneous" tab of a traditional paper record, which has become the "kitchen junk drawer" of the medical records department.

With increasing numbers of providers converting to electronic health records (EHR), the question of how—and whether—to address and integrate these records into the facility's medical records is becoming more difficult and more labor-intensive, particularly when such information needs to be scanned, keyed, or otherwise incorporated into the EHR. Here are some things to consider.

Other than records a healthcare provider receives when a patient is transferred from another provider (such as records transferred due to an EMTALA obligation, EMS records, and records received pursuant to obligations in a transfer agreement or pursuant to a referral), healthcare providers are under no general legal obligation to accept health records from any outside sources. A provider might want to review and use those records to provide better or more complete patient care, but it does

not have to. And due to current payment methods for providers, there is actually a perverse disincentive not to use records of previous care if providers can retest or re-examine a patient and get paid for it.

It is also important to note that not all personal health records (PHRs) are equal; some have inherent indicia of reliability, whereas others do not. If a healthcare provider accepts medical records from outside sources, it must have a protocol to help determine whether each record was actually used by a clinician in developing the plan of care or in treating the patient. In the paper environment, it is (relatively) easy for a clinician to indicate whether he or she reviewed an external record of care. In the electronic environment, however, it is almost impossible to do so, particularly when the external information comes preloaded on a flash drive or compact disc that has its own loading and viewing software—both of which are formats increasing in popularity with PHR users.

Whether a healthcare provider has accessed records of a patient's previous care via the Internet is also virtually impossible to determine, but this question is qualitatively different as such information never really becomes resident on the viewing clinician's computer, but instead resides in cyberspace when being viewed. Providers should consider adopting a policy that requires clinicians to make an entry in the medical record noting his investigation of this remote PHR and identifying any useful data that he derived therefrom. And, to the extent that the useful data can be incorporated into the medical record, it should be.

If a healthcare provider cannot adopt a policy that requires clinicians to indicate whether and what portion of outside records the clinician has used, or if the kinds of outside records it is receiving are not capable of showing use, then unfortunately it is recommended that the provider treat all of the information that is available for inclusion in the patient record as being used by the clinician and include it in the official patient record as if it were information specifically requested from an outside source (such as a laboratory test or a radiological interpretation). Depending on state law and the provider's own policies, this in turn would mean that the provider could be required to disclose this outside information pursuant to a patient request or some external legal process (see the discussion above about redisclosure). This also means that the facility and the clinicians treating the patient will be charged with knowledge of this information should any risk management or malpractice scenarios arise.

Trial Subpoenas vs. Discovery Subpoenas

There is a common belief among the healthcare community that subpoenas calling for testimony or documents to be produced at trial do not need to comply with HIPAA. This misconception likely stems from the notion that the elicitation of testimony or disclosure of documents in a courtroom and in the presence of a judge is implicitly sanctioned or required by the judge. This is simply not the case.

In the absence of a valid authorization, HIPAA permits the disclosure of protected health information in response to a subpoena only if the subpoena is accompanied by an order, or the covered entity receives satisfactory assurances that reasonable efforts have been made to either (1) secure a qualified protective order, or (2) give the patient notice of the subpoena, and the patient has not objected (as stated in 45 C.F.R. 164.512(e)(ii)).

HIPAA makes no distinction between subpoenas issued for purposes of trial and those issued for purposes of obtaining pre-trial discovery. Disclosure of protected health information, even in the presence of a judge, must be accompanied by either the satisfactory assurances discussed above or a valid authorization. Attorneys and HIM professionals have seen some tortured logic that tries to classify these subpoenas as orders, thereby forcing them under the provisions of 45 C.F.R. 164.512 (e)(1)(i). However, even these types of subpoenas may be challenged in open court and production of information conditioned on a ruling from the judge (i.e., an order). A subpoena is not an order for purposes of the HIPAA Privacy Rule.

Thoughts for Process Improvement

Compliance lawyers hate the concept of "peer benchmarking," which is basically just comparing yourself to how well (or poorly) others comply with the law. The only real benchmark in the compliance game is 100 percent compliance. Let's focus instead on processes that you can adopt that help you comply with the legal issues created in these scenarios:

- Have your counsel prepare a checklist or bullet point summary of the different types of requests your department is likely to receive in litigation matters, and use the checklist to decide when you need to call counsel. Often, there are

simple strategies you can employ to determine whether a subpoena or another type of request (i.e., workers' compensation, OSHA, military, etc.) comply with applicable law.

- Go back through the exercise of defining the official patient record. Develop a policy concerning the acceptance and use of records generated outside of the practice or facility, including those volunteered by patients or their representatives. Check with your local counsel to make sure that specific state law does not treat these records differently.
- Be prepared to disclose the entire official patient record upon request, subject only to restrictions imposed by law. The fact that the record originated outside of your facility or practice is not a reason to withhold disclosure.
- Develop a policy concerning the treatment of unaccompanied minors in non-emergency situations (being mindful of any Medicaid requirements in your state).
- Develop a script or document that explains to minors who self-refer for treatment the privacy implications of billing their parents' insurance.
- Develop a procedure to tag or classify records of minor patients so that, when the date of the patient's majority is reached, the parent or guardian no longer is shown as a responsible party or is capable of accessing the record.
- If a record is not used in the treatment, management, care, etc. of a patient, seriously rethink why that record is being kept as a part of the official record of patient care.

Barry S. Herrin (barry.herrin@herrinhealthlaw.com) is founder of Herrin Health Law, P.C. The information contained in this article is for general information of the reading public and is not to be considered legal advice.

Article citation:
Herrin, Barry S.. "Release of Information: When to Call a Healthcare Compliance Attorney" *Journal of AHIMA* 87, no.9 (September 2016): 24-27.