Federal Regulations and Guidelines for Client Access to Records

written by Guest Author | July 22, 2016

*__An earlier version of the article did not include a statement that the definition of a "covered entity" was applicable to Texas Mental Health Professional guidelines. Texas has expanded the definition of covered entity to include any provider who receives, transmits or stores PHI in electronic format for any reason or purpose. Any email or text messaging that a Texas MHP participates in will cause a Texas MHP to be a covered entity for Privacy Rule purposes.__

I have spoken with literally thousands of mental health professionals (mhps) during my career as a lawyer that have been faced with a request for records. I wish I had five dollars for the number of times I was told by a mhp, "I never give out copies of my records, I only provide summaries." I have had a difficult time convincing many of them that their clients were entitled to obtain copies of their records.

The US Department Of Health and Human Services has published guidelines for individuals' right under HIPAA to access their health information (45 CFR §164.24). The thinking behind the Department's regulations and guidelines is to provide individuals with ***easy access*** to their health information to empower them to be more in control of decisions regarding their health and well-being. This will allow individuals to better monitor their conditions, adhere to treatment plans, find and fix errors in their health records, track progress in wellness or disease management programs, and directly contribute their information to research. The goal is to put individuals in the driver's seat with respect to their health as we move toward a more patient-centered health care system.

The bottom line is that individuals have a right to review and obtain copies of their records. Summaries can only be provided if the client requests one or agrees to accept the summary in lieu of the copies. "Records" means any item, collection or grouping of information that includes protected health information (PHI) and is maintained, collected, used, or disseminated by or for a covered entity. I have had many mhps tell me that they are not a covered entity because they keep paper records so they do not have to worry about HIPAA. I then ask them if they have you ever communicated with a client by email or text messaging. I have never had any one tell me they have not. Those electronic communications with your clients make you a covered entity.

A mhp is allowed to withhold psychotherapy notes from review by a client. These are defined as notes a mhp records in a separate file from the client's clinical file about the communications shared between the client and the provider that are for the provider's use only. Many mhps tell me that they will not turn over their notes thinking the psychotherapy note exception applies. When I ask them if they keep these notes in a separate file I am often told that they do not. If not, then they are not psychotherapy

notes as defined by the regulations. In some states, such as California and Minnesota, clients are allowed under state law to access psychotherapy notes and they cannot be withheld from a client. Generally, where a state law provides better privacy protection or greater access to records" state law will supersede federal law.

The regulations allow a mhp to also withhold information under the following circumstances:

- If any portion of the requested record is **reasonably likely to endanger the life or physical safety of the individual or another person**. This ground for denial does not extend to concerns about psychological or emotional harm (e.g., concerns that the individual will not be able to understand the information or may be upset by it).
- If any portion of the requested record is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
- If a personal representative (i.e. parent) has requested access and any portion of the requested record is reasonably likely to cause substantial harm to the individual (i.e. child) or another person (i.e. the other parent).

These rules are game changers for mhps in states like Texas that that allow for denial of information based on professional judgment that disclosure would be harmful to the patient's physical, mental, or emotional health. Under the Federal regulations and guidelines concern for emotional health would not constitute a basis unless the mhp could tie it to some risk to life or physical safety like an increased risk of suicide. It would be important for that risk to be evident from the face of the records themselves in the event a complaint were filed with a state licensing board or the Office of Civil Rights.

Many mhps have shared their sincere concern about allowing a parent to access his or her child's records on the belief that it will destroy the child's trust in the therapist and for all future therapists. Based on the regulations and guidelines now in place that will not constitute a basis for withholding the information from the parent unless the mhp can make a valid connection to endangerment to life or physical safety.

The regulations and guidelines require all other information that is not reasonably likely to endanger life or physical safety be provided. This would require redacting from the record copy only the information reasonably likely to endanger life or physical safety.

All requests for information must be responded to within thirty (30) days and if a state law requires an earlier response time the state time period will apply. The thirty (30) day rule is described as the maximum window and if a provider has an electronic record system that allows for quick dissemination of records it would be improper for the provider to withhold the information for the full thirty days.

If the provider cannot comply with the request within 30 days for a valid reason such as offsite storage, then the response period can be extended for no more that an additional 30 days but written notice must be provided within the first thirty (30) day window.

If a covered entity denies access, in whole or in part, to PHI requested by the individual, the covered entity must provide a denial in writing within thirty (30) days (or sixty (60) days if the time period is extended) that:

- is in plain language;
- describes the basis for denial;
- informs the individual of the right to have the decision reviewed and how to request such a review; (denial of psychotherapy notes is not reviewable) and
- informs the individual he or she may submit a complaint to the covered entity or the HHS Office for Civil Rights.

Other key rules to keep in mind when faced with a records request are:

- A covered entity may not deny access because a business associate of the covered entity, rather than the covered entity itself, maintains the PHI requested by the individual (e.g., the PHI is maintained by the covered entity's electronic health record vendor or is maintained by a records storage company offsite).
- A covered entity may not require an individual to provide a reason for requesting access, and the individual's rationale for requesting access, if voluntarily offered or known by the covered entity or business associate, is not a permitted reason to deny access.
- Clients have the right to access all the information maintained in their file even if it was received from a third party (i.e. psychologist report).
- A covered entity also may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided in addition to that PHI, so long as the individual in advance: (1) chooses to receive the summary or explanation (including in the electronic or paper form being offered by the covered entity); and (2) agrees to any permitted fees.
- A client can request electronic or paper copies of records. If the covered entity does not maintain electronic records but has a scanner and can "readily scan the paper record into an electronic format" the covered entity must do so.
- A covered entity also must provide access in the manner requested by the individual, which includes arranging with the individual for a convenient time and place to pick up a copy of the PHI or to inspect the PHI (if that is the manner of access requested by the individual), or to have a copy of the PHI mailed or e-mailed, or otherwise transferred or transmitted to the individual to the extent the copy would be readily producible in such a manner.
- A covered entity is not expected to tolerate unacceptable levels of risk to the security of the PHI on its systems in responding to requests for access; whether the individual's requested mode of transfer or transmission presents such an unacceptable level of risk will depend on the covered entity's Security Rule risk analysis. However, mail and e-mail are generally considered readily producible by all covered entities. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail (except in the limited case where e-mail cannot accommodate the file size of requested images), and transmitting PHI in such a manner does not present

unacceptable security risks to the systems of covered entities, even though there may be security risks to the PHI **while in transit** (such as where an individual has requested to receive her PHI by, and accepted the risks associated with, unencrypted e-mail). Thus, a covered entity may not require that an individual travel to the covered entity's physical location to pick up a copy of her PHI if the individual requests that the copy be mailed or e-mailed.

- A covered entity may require individuals to request access in writing, provided the covered entity informs individuals of this requirement. Covered entities also may offer individuals the option of using electronic means (e.g., e-mail, secure web portal) to make requests for access. In addition, a covered entity may require individuals to use the entity's own supplied form, provided use of the form does not create a barrier to or unreasonably delay the individual from obtaining access to his PHI.
- A covered entity must take reasonable steps to verify the identity of an individual making a request for access. No particular form of verification (such as obtaining a copy of a driver's license) is mandated, but rather generally leaves the type and manner of the verification to the discretion and professional judgment of the covered entity, provided the verification processes and measures do not create barriers to or unreasonably delay the individual from obtaining access to her PHI, as described below.
- A covered entity may impose a reasonable, cost-based fee if the individual requests a copy of the PHI (or agrees to receive a summary or explanation of the information). The fee may include only the cost of: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media; (3) postage, when the individual requests that the copy, or the summary or explanation, be mailed; and (4) preparation of an explanation or summary of the PHI, if agreed to by the individual. The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by State law.

In summary, it has become more difficult to keep clients from accessing their records. The regulations and guidelines pose many technical requirements that can trip up a well- meaning mhp when a client seeks access to their records. It is imperative to document in writing all your communications with clients about their records i and to note and pay attention to dates and time periods. Mhps should thoughtfully review their policies and practices with respect to content recorded in a client file. Less may not always be better if one has to defend a denial of information to a client.

Written by Tom L. Hartsell, Attorney at Law