

Managing Exceptions to HIPAA's Patient Access Rule

Save to myBoK

by Gwen Hughes

The HIPAA final privacy rule requires that covered entities allow individuals to access the medical and billing records maintained about them. However, the rule describes 10 exceptions. Accordingly, healthcare providers must establish a way to identify the medical and billing records to which these exceptions to access apply.

Exceptions to Remember

The HIPAA privacy rule grants individuals the right to information about them in a designated record set. The rule goes on to define designated record set as medical and billing records maintained by or for the covered entity to make decisions about these individuals. If information is not part of the designated record set, then according to HIPAA, an individual's request for such information can be denied.

The rule specifically addresses two types of such information:

1. **Psychotherapy notes:** Recorded by a mental health professional and maintained separately from the rest of the medical record, psychotherapy notes document or analyze conversation during a private or group counseling session. By definition, psychotherapy notes do not include medication records, counseling start and stop times, treatment records, results of clinical tests, diagnoses, functional status, symptoms, prognosis and progress, and psychotherapy notes maintained within the individual's regular health record.
2. **Information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding:** In many organizations, for example, incident reports are generated when a patient falls or a medication is given in error. These reports are used to identify problems, implement corrective action, and to respond to civil, criminal, or administrative action. Although pieces of the information in the incident report such as the patient's condition are recorded in the patient's health record, incident reports are filed in separate administrative or legal files.

The HIPAA privacy rule describes a third access exception that applies to information originated and maintained in laboratories:

3. **Information Subject to the Clinical Laboratory Improvement Amendments of 1988 (CLIA).**¹ Labs that are subject to CLIA must not grant patients access to test results if CLIA bans them from doing so. Research labs that are exempt from CLIA may also deny patients access to health information.²

If HIPAA limited exceptions only to psychotherapy notes, reports made in anticipation of legal action, and the release of test results by laboratories, covered entities would find it unnecessary to flag exceptions. Such exceptions would be relatively easy to manage. However, the next seven HIPAA exceptions describe specific scenarios that are more difficult to handle:

4. **The patient is an inmate** and obtaining a copy of his health information would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates, the safety of an officer, employee, other person at the correctional institution, or individual responsible for transporting the inmate.
5. **The individual previously agreed to a temporary denial of access** while part of a research project that includes treatment. The temporary denial of access applies as long as the research is in progress.
6. **The individual's access to protected health information is subject to and may be denied under the Privacy Act of 1974.**³ The act applies to record systems operated by the federal government or pursuant to a contract with a government agency. The act therefore applies to information maintained in military hospitals and veterans administration and Indian health services.
7. The protected health information was **obtained from someone other than a healthcare provider under a promise of confidentiality**, and access would likely reveal the source of the information.

8. A licensed healthcare professional has determined that **the access requested is likely to endanger the life or physical safety of the individual or another person.**
9. The **protected health information makes reference to another person** (unless the other person is a healthcare provider) and a licensed healthcare professional has determined that access is likely to cause substantial harm to the other person.
10. The request for access is made by the individual's personal representative and a licensed healthcare professional has determined access is likely to **cause substantial harm to the individual or another person.**

Identifying the Exceptions

Identifying records to which the psychotherapy, legal proceeding, and laboratory exceptions apply is relatively simple. Identifying information or records to which the seven case-specific exceptions apply is more complex. So how can providers best flag these exceptions?

There are a number of possibilities:

1. **Providers from whom access is requested can contact the attending physician whenever an individual requests access.** In many settings, however, this is not a practical solution. There are numerous requests, the physician is busy, and recollection of information about the individual can be vague.
2. **The individual or office charged with disclosure can read through every record entry looking for exceptions prior to disclosure.** Again, this is not a practical solution in many settings. There are numerous requests, the ability to read the records is limited, and there are little or no human resources available to take on this responsibility.
3. **Providers can use a color-coded label** applied in a standard location on the chart or at the site of specific entries to highlight particularly sensitive information of which release to the individual or his legal representative may be inappropriate. This solution is fairly easy to implement, but not 100 percent accurate. Should sites decide to use this type of flagging solution, HIM professionals should anticipate questions by individuals about the meaning of the color-coded labels and train staff to give the appropriate response.
4. **Providers can designate a location on the face sheet, problem list, or file folder on which the date of any sensitive entry can be recorded.** The advantage of this particular method is that it can be done in a way that is more discrete than some other methods of flagging exceptions.
5. **Providers can generate a "Disclosure Restriction Form."** (See [Sample](#)). Such a form might contain the patient's name, record number, entries to which access should be denied, the individual or personal representative to whom access should be denied, the duration the denial should be in place, and the signature and date of the individual generating the form. The form can be sent to the HIM department to be maintained in a paper or electronic database. While the individual is an inpatient, requests for access can be routed through the attending physician. Thereafter, staff charged with the responsibility of processing disclosures can check requests against disclosure restrictions forms maintained in a notebook, other paper file, or computer database.

HIM professionals can find it challenging to identify health record entries or circumstances in which it may be inappropriate to disclose information to the individual or the individual's legal representative. While there is a myriad of information, there are often just a few cases in which access needs to be denied. Nevertheless, it's important to develop a system for identifying entries that should not be disclosed. The disclosure restriction form or one of the other tools identified above may be the right solution for your organization.

Notes

1. Clinical Laboratory Improvement Amendments of 1998, 42 USC 263a.
2. "Laboratory Requirements." 42 CFR 493(a)(2)
3. Privacy Act of 1974, 5USC 522a.

References

- Abdelhak, Mervat et al. *Health Information: Management of a Strategic Resource*. Philadelphia: W.B. Saunders, 1996.

- "Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 65, no. 250 (December 28, 2000). Available at <http://aspe.hhs.gov/admnsimp>.

Gwen Hughes (gwen.hughes@ahima.org) is an HIM practice manager at AHIMA

Article citation:

Hughes, Gwen. "Managing Exceptions to HIPAA's Patient Access Rule." *Journal of AHIMA* 72, no.9 (2001): 90-92.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.