Shumaker

MAY 6, 2026 | PUBLICATION

Client Alert: The Government May Actually Be Here to Help - Health Insurance Portability and Accountability Act of 1996 (HIPAA) Part VI

INDUSTRY SECTOR

Health Care

SERVICE LINE

Health Law

RELATED PROFESSIONALS

Grant P. Dearborn
Katherine H. Crawford

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The United States Department of Health and Human Services (HHS) provides a helpful set of questions and answers on its website regarding the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Professionals should note that this guidance is informal, may be updated or withdrawn, and may differ from state laws. Below, we highlight three questions and answers from the HHS website.

Does an individual have a right to access all of the information a covered entity maintains in the individual's medical record?

Except in very limited circumstances, an individual has a right to access all personal health information (PHI) about the individual that a covered entity (or its business associate) maintains in one or more designated record sets. A designated record set is defined to include the medical record about the individual. Thus, an individual generally has a right to access all of the information about the individual that a covered entity maintains in the individual's medical record, including information the individual provided to the covered entity herself, as well as PHI about the individual contributed to the record by other health care providers or covered entities. See 45 CFR 164.524(a)(2) – (a)(3) for the limited grounds upon which a covered entity may deny an individual access to PHI in a designated record set.

Content reviewed last June 24, 2026

Under what circumstances may a covered entity deny an individual's request for access to the individual's PHI?

A covered entity may deny an individual access to all, or a portion of the PHI requested in only very limited circumstances. For example, a covered entity may deny an individual access if the information requested is not part of a designated record set maintained by the covered entity (or by a business associate for a covered entity), or the information is excepted from the right of access because it is psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a legal proceeding (but the individual retains the right to access the underlying PHI from the designated record set(s) about the individual used to generate this information).

Another limited ground for denial exists if a licensed health care professional determines in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. For example, a covered entity may deny a suicidal patient access to information that a provider determines in his professional judgment is reasonably likely to lead the patient to take her own life. However, we stress that this ground is narrowly construed in order to protect individuals' autonomy interests and their right under the Privacy Rule to obtain information about themselves, which is fundamental in facilitating individuals' active participation in their own health care. General concerns about psychological or emotional harm are not sufficient to deny an individual access (e.g., concerns that the individual will not be able to understand the information or may be upset by it). In addition, the requested access must be reasonably likely to cause harm or endanger physical life or safety. Thus, concerns based on the mere possibility of harm are not sufficient to deny access. As a result, we expect this ground for denial to apply in extremely rare circumstances. Further, an individual who is denied access based on these grounds has a right to have the denial reviewed by a licensed health care professional designated by the covered entity as a reviewing official who did not participate in the original decision to deny access.

For a complete list of the grounds and conditions for denial of access, see 45 CFR 164.524(a)(2)-(4). Note that an individual may not be required 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.

If a covered entity denies access, in whole or in part, to PHI requested by the individual based on one or more permitted grounds, the covered entity must provide a denial in writing to the individual no later than 30 calendar days after the request (or no more than 60 calendar days if the covered entity notified the individual of an extension). See 45 CFR 164.524(b)(2). The denial must be in plain language and describe the basis for denial; if applicable, the individual's right to have the decision reviewed and how to request such a review; and how the individual may submit a complaint to the covered entity or the HHS Office for Civil Rights. See 45 CFR 164.524(d).

The covered entity must, to the extent possible, provide the individual with access to any other PHI requested, after excluding the PHI to which the entity has a ground to deny access. See 45 CFR 164.524(d)(1).

Content reviewed last June 24, 2026

How timely must a covered entity be in responding to individuals' request for access to their PHI?

Under the HIPAA Privacy Rule, a covered entity must act on an individual's request for access no later than 30 calendar days after receipt of the request. If the covered entity is not able to act within this timeframe, the entity may have up to an additional 30 calendar days, as long as it provides the individual–within that initial 30-day period–with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request. See 45 CFR 164.524(b)(2).

These timelines apply regardless of whether:

- The PHI that is the subject of the request is maintained by the covered entity or by a business associate on behalf of the covered entity, or the covered entity uses a business associate to fulfill individual requests for access. The 30-day clock starts on the date that the covered entity receives a request for access, so any delay in obtaining the necessary information from a business associate or forwarding the request to the business associate for action "uses up" part of the allotted time. Alternatively, the 30-day clock starts when, instead of the covered entity, a business associate receives a request directly from an individual because the covered entity instructed the individual through its notice of privacy practices (or otherwise) to submit the access request directly to its business associate for processing.
- The covered entity negotiates with the individual on the format of the response. Covered entities that spend significant time before reaching agreement with individuals on format are depleting the 30 days allotted for the response by that amount of time.
- The PHI that is the subject of the request is old, archived, and/or not otherwise readily accessible.

These timelines are outer limits, and it is expected that many covered entities should be able to respond to requests for access well before these outer limits are reached. However, in cases where a covered entity is aware that an access request may take close to these outer time limits to fulfill, the entity is encouraged to provide the requested information in pieces as it becomes available, if the individual indicates a desire to receive the information in such a manner.

Content reviewed last June 24, 2016

Health care providers may require that patient requests for access to their medical records be made in writing. However, they must provide patients with notice of this requirement. We recommend that providers establish and maintain a clear policy for handling these requests. As stated above, once a patient makes a request to view their medical record, the covered entity has 30 calendar days to comply with the request. If this timeframe is not feasible, the entity may have up to an additional 30 calendar days to provide access, but only if the entity provides the patient within the initial 30-day window with a written explanation for the delay and the date by which the access will be granted. If a provider is contemplating denying a patient's request for access, we highly recommend the provider review the limited grounds for denial set forth in the Privacy Rule to ensure such denial is warranted and to mitigate risk that a patient later submits a complaint to HHS against the provider.

For more information, please contact Grant Dearborn, Kate Crawford, or another member of Shumaker's Health Law Service Line.