Guidance on HIPAA and Individual Authorization of Uses and Disclosures of Protected Health Information for Research

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

21st Century Cures Act of 2016 (Cures Act) Mandate

The Cures Act requires the Secretary of the Department of Health and Human Services (HHS) to issue "Guidance Related to Streamlining Authorization" under HIPAA for uses and disclosures of protected health information (PHI) for research.[1, 2] Specifically, the guidance must clarify:

(1) the circumstances under which the authorization for use or disclosure of protected health information, with respect to an individual, for future research purposes contains a sufficient description of the purpose of the use or disclosure, such as if the authorization
  (A) sufficiently describes the purposes such that it would be reasonable for the individual to expect that the protected health information could be used or disclosed for such future research,
  (B) either
    (i) states that the authorization will expire on a particular date or on the occurrence of a particular event or
    (ii) states that the authorization will remain valid unless and until it is revoked by the individual, and
  (C) provides instruction to the individual on how to revoke such authorization at any time;
(2) the circumstances under which it is appropriate to provide an individual with an annual notice or reminder that the individual has the right to revoke such authorization; and
(3) appropriate mechanisms by which an individual may revoke an authorization for future research purposes, such as described in paragraph (1)(C).

The HHS Office for Civil Rights (OCR) provides the following guidance, consisting of background on the HIPAA Privacy Rule's provisions on authorizations to use and disclose PHI for research and detailed discussion of each of the three topics identified in the Cures Act.

Background

HIPAA protects the privacy of individually identifiable health information known as "protected health information" (PHI). The Privacy Rule provides that covered entities and business associates may use or disclose PHI, including for research purposes, only as permitted or required by the Privacy Rule or as authorized in writing by the individual who is the subject of the information (or by the individual's personal representative). At the same time, the Privacy Rule helps ensure that researchers are able to access PHI needed to conduct vital research. While the Privacy Rule does permit certain uses and disclosures of PHI for research purposes without

[1] Pub. L. 114-255, section 2063(b).
[2] "Research" is defined in the Privacy Rule as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." See 45 CFR § 164.501.

an individual's authorization,[3] this document focuses specifically on situations in which an entity obtains the individual's HIPAA authorization for uses and disclosures of PHI for research.

General Authorization Requirements and Expiration of Authorizations

HIPAA-compliant authorizations must be in plain language and contain specific information regarding: a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion, the names or other specific identification of the persons authorized to disclose and receive the information, a description of each purpose of the requested use or disclosure, and an expiration date or expiration event that relates to the individual or the purpose of the use or disclosure. HIPAA-compliant authorizations must also include statements adequate to place the individual on notice of all of the following: (1) the individual's right to revoke the authorization in writing; any exceptions to the right to revoke the authorization and a description of how the individual may revoke the authorization or, if such information is included in the notice required by 45 CFR § 164.520, a reference to the covered entity's notice; (2) the ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization; and (3) the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by the HIPAA Privacy Rule.[4]

Guidance on Sufficient Descriptions of the Purpose of a Use or Disclosure for Future Research Authorizations

OCR presents the following guidance on the circumstances in which an authorization for uses and disclosures of PHI for future research contains a sufficient description of the purpose of the use or disclosure being authorized. In accordance with section 2063(b)(1)(A) of the Cures Act, this guidance explains what form of description of future research, consistent with the interpretation provided in the preamble to the Omnibus HIPAA Final Rule,[5] is sufficient to comply with 45 CFR § 164.508(c)(1)(iv). While OCR desires to provide timely guidance for researchers, it also believes it would be helpful to have additional insight into, and input on, the complex question of what constitutes a sufficient description such that it would be reasonable for the individual to expect that the PHI could be used or disclosed for such research. Accordingly, the following guidance on this issue is interim guidance, while additional inquiries and discussions proceed.

Authorizations for the use or disclosure of PHI for future research (or other purposes) must include a "description of each purpose of the requested use or disclosure. The statement 'at the request of the individual' is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose." [6]

[3] More information on the HIPAA Privacy Rule and research is available on OCR's website at https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html.
[4] See 45 CFR § 164.508(c).
[5] See 78 Fed. Reg. 5566, 5611–5613 (Jan. 25, 2013).
[6] See 45 CFR § 164.508(c)(1)(iv).

In the preamble to the Omnibus HIPAA Final Rule, OCR stated that, with regard to future research authorizations, the requirement to describe "each purpose" means that such authorizations do not need to specify each specific future study if the particular studies to be conducted are not yet determined; rather, the authorization "must adequately describe such purposes such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research." [7]

In short, OCR views a description of future research purposes as compliant with 45 CFR § 164.508(c)(1)(iv) if the description sufficiently describes the purposes such that it would be reasonable for the individual to expect that the protected health information could be used or disclosed for such future research.

Guidance on the Expiration of Authorizations for Future Research

Pursuant to sections 2063(b)(1)(B) and (C) of the Cures Act, OCR clarifies that an authorization for uses and disclosures of PHI for future research must contain "an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure." [8] When, as here, the authorization is for a use or disclosure of PHI for research, "including for the creation and maintenance of a research database or research repository," "the statement 'end of the research study,' 'none,' or similar language is sufficient." [9] One example of such a permissible "expiration event that relates to the individual" would be if the authorization states that the authorization will remain valid unless and until it is revoked by the individual.

Guidance on the Right to Revoke Authorization

The HIPAA Privacy Rule establishes an individual right to revoke an authorization for uses and disclosures of PHI for research, in writing, at any time, except to the extent that the covered entity has taken action in reliance on the authorization.[10] To be valid, an authorization must inform the individual of the right to revoke the authorization in writing, and either: (1) the exceptions to the right to revoke and a description of how the individual may revoke authorization, or (2) reference to the corresponding section(s) of the covered entity's Notice of Privacy Practices.[11]

A HIPAA authorization can allow a covered entity to use or disclose an individual's PHI for its own research purposes or disclose PHI to another entity for that entity's research activities. Thus, revocation of an authorization limits a covered entity's own continued use of the health information for research that was conducted based on the authorization, and prevents the covered entity from making future disclosures for research purposes based on the authorization.[12]

[7] See 78 Fed. Reg. 5566, 5612 (Jan. 25, 2013).
[8] See 45 CFR § 164.508(c)(1)(v).
[9] Id.
[10] See 45 CFR § 164.508(b)(5).
[11] See 45 CFR § 164.508(c)(2).
[12] See 45 CFR § 164.508(b)(2) (An authorization that has been revoked is a defective authorization.).

However, individuals should be aware that revocation of an authorization does not always mean that the individual's information may no longer be used in the research study or may no longer be used or disclosed for any other purpose. A covered entity may continue to use and disclose PHI that was obtained before the individual revoked authorization to the extent that the entity has taken action in reliance on the authorization.[13] In cases where the research is conducted by the covered entity, the exception to revocation would permit the covered entity to continue using or disclosing the PHI to the extent necessary to maintain the integrity of the research—for example, to account for a subject's withdrawal from the research study, to conduct investigations of scientific misconduct, or to report adverse events. A covered entity also could continue to use the PHI for other activities that would be permitted by the Privacy Rule without the individual's authorization. For example, a covered entity could disclose PHI it collected for research purposes to conduct permitted health care operations, such as quality assessment and improvement activities.[14]

Reminder of the Right to Revoke

The Privacy Rule does not require a covered entity to provide periodic reminders about an individual's right to revoke an authorization. Instead, the Privacy Rule requires such entities to provide individuals with a copy of their signed authorization to ensure the individual is aware of the ongoing potential for the uses and disclosures of PHI pursuant to an authorization that has not expired.

While not required, a covered entity may provide reminders to individuals of their right to revoke a research authorization. For example, a covered entity might choose to ask, while obtaining an individual's authorization, whether the individual would like to receive reminder(s) in the future about the right to revoke the authorization and, in accordance with such request, provide periodic reminders of such right to revoke. Or, a covered entity might remind a minor participant who reaches the age of majority of their right to revoke a HIPAA authorization originally signed by the minor's personal representative (usually a parent or guardian). Reminders of this nature are not, however, required under the Privacy Rule.

Appropriate Methods for Revoking Authorization for Future Research

In addition to clearly stating that an individual has a right to revoke an authorization in writing at any time, the authorization must describe the process by which an individual may revoke the authorization, which may be accomplished in paper or electronic form.[15] In circumstances where a covered entity's Notice of Privacy Practices contains a clear description of the revocation process, the authorization can refer to this information in the Notice of Privacy Practices.[16]

The Privacy Rule does not prevent covered entities from establishing reasonable procedures for revocation, such as providing a standard revocation form. Covered entities are encouraged to establish processes that facilitate an individual's exercising the right to revoke an authorization.

[13] See 45 CFR § 164.508(b)(5)(i).
[14] See the definition of "Health care operations" at 45 CFR § 164.501 and 45 CFR § 164.506.
[15] See 45 CFR § 164.508(c)(2)(i)(A).
[16] See 45 CFR § 164.508(c)(2)(i)(B).

For example, a covered entity could make authorizations currently in effect viewable by the individual through an electronic health record portal and allow the individual to submit revocations through the portal.

Once signed, a revocation is not effective until the covered entity that would rely on the authorization receives the revocation or has knowledge of the revocation.[17] The existence of a written revocation of authorization does not always mean that a covered entity has ''knowledge'' of the revocation that would make the authorization defective.[18] Conversely, obtaining a copy of the written revocation is not required before a provider ''knows'' that an authorization has been revoked.[19]

To illustrate these points, consider a situation in which a person other than a covered entity making the disclosure obtains an individual's authorization, which it then presents to such covered entity, thus allowing the covered entity to disclose PHI. If the individual revokes the authorization by writing to that non-disclosing person who obtained the authorization, and neither the individual nor the other person informs the disclosing covered entity of the revocation, that covered entity will not ''know'' that the authorization has been revoked. For example, a non-HIPAA covered researcher studying cardiac health might obtain an individual's authorization for ''all providers who have seen the individual in the past year'' to disclose PHI related to the individual's heart condition. Later, the individual may decide to revoke the authorization by writing to the researcher requesting such revocation. The Privacy Rule does not require the researcher in this example to inform all covered entities to whom it has presented the authorization that the authorization has been revoked, so one or more disclosing providers may not "know." At the same time, however, if the individual tells a covered entity that the individual has revoked the authorization in writing to the researcher, the covered entity ''knows'' of the revocation and must consider the authorization defective (*i.e.*, invalid) under § 164.508(b)(2).[20]

Finally, a covered entity is permitted, but not required, to use or disclose PHI subject to an authorization. Thus, while the Privacy Rule requires that a revocation of authorization be in writing, a covered entity may choose to cease using and disclosing PHI pursuant to an authorization based on an individual's oral request if the covered entity chooses to do so.[21]

[17] See 65 Fed. Reg. 82462, 82515 (December 28, 2000).
[18] Id.
[19] Id.
[20] Id.
[21] See 78 Fed. Reg. 5566, 5613 (January 25, 2013).