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

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 Authorizations" 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 and disclosure of PHI for future research purposes contains a sufficient description of the purpose of the use or disclosure;
(2) the circumstances under which it is appropriate to provide an individual with an annual notice or reminder of the right to revoke an authorization; and
(3) appropriate mechanisms by which an individual may revoke an authorization for future research purposes.

The guidance below provides background on the HIPAA Privacy Rule with respect to authorizations for uses and disclosures of PHI for research, and then addresses each of the three topics identified in the Cures Act in detail.

Background

HIPAA protects the privacy of individually identifiable health information by providing 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 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 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

[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.
[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.

HIPAA-compliant authorizations must be in plain language and contain specific information regarding: the information to be disclosed or used, the persons disclosing and receiving the information, the purpose(s) of the requested use or disclosure, when the authorization expires, a statement about the individual's right to revoke the authorization in writing, and other information individuals need to know about what will happen to their information and about their rights with respect to the information.[4]

In accordance with sections 2063(b)(1)(B) and (C) of the Cures Act, we clarify that an authorization for uses and disclosures of PHI for future research must contain a statement that the authorization will expire on either a particular date or an expiration event related to the individual or the purpose of the use or disclosure.[5]This statement could be: "end of the research study," "none," "unless and until revoked by the individual," or something similar.

Guidance on HIPAA Authorizations for Future Research and the Description of the Purpose of the Use or Disclosure Being Authorized

This section of guidance outlines OCR's views regarding 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), this guidance explains OCR's expectations for covered entities regarding the description of future research, which are consistent with the interpretation provided in the preamble to the Omnibus HIPAA Final Rule.[6] OCR believes it would be helpful to have additional insight regarding 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; therefore, OCR is issuing the below portion of the guidance as interim guidance while additional research and discussions proceed. OCR will work with federal partners in HHS to identify the best way to obtain this insight, which we will take into consideration in future guidance on this topic.

Authorizations that are obtained for the use or disclosure of PHI for research (or other purposes) must describe the purpose(s) of the use or disclosure. Often, an authorization will specify a particular research study that will continue for a set period of time and conclude without an ongoing or future need to use or disclose the PHI. In other circumstances, a covered entity may request an authorization to use or disclose health information for a current research study as well as for future research. For example, a covered entity conducting a research study may want to include PHI collected from the individual in a research database or repository to be used for future research. In some cases, this may occur in conjunction with a clinical trial, such as when information obtained from a research participant during the trial is transferred to and maintained in a research database or repository of information about individuals who have a particular health condition.

[4] See 45 CFR § 164.508(c).
[5] See 45 CFR § 164.508(c)(1)(v).
[6] See 78 Fed. Reg. 5566, 5611-5613 (January 25, 2013).

The Privacy Rule does not require that a research authorization describe each specific future study if the particular studies to be conducted are not yet determined. Instead, to satisfy the requirement that an authorization include a description of each purpose of the requested use or disclosure, an authorization for use and disclosure of PHI for future research purposes must adequately describe future purposes such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research.[7] For example, the description could include specific statements with respect to whether sensitive research, such as genetic or mental health research, or is contemplated. However, the Privacy Rule does not prescribe a fixed level of detail about the future research or identify particular types of PHI as "sensitive."

In short, the Privacy Rule gives covered entities and researchers (who may or may not be covered by HIPAA) the flexibility to describe the future research and the health information to be used or disclosed for the future research, so long as such description reasonably puts the individual on notice that his or her protected health information could be used or disclosed for the future research.

As indicated in the introduction to this section, OCR, in collaboration with federal partners, will continue to explore aspects of this particular issue as we continue developing this part of the guidance.

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.[8] 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.[9]

A HIPAA authorization allows 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 based on the authorization.[10]

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 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

[7] A HIPAA authorization for future research also must address each of the core elements and statements required at 45 CFR § 164.508(c).
[8] See 45 CFR § 164.508(b)(5).
[9] See 45 CFR § 164.508(c)(2).
[10] See 45 CFR § 164.508(b)(2) (An authorization that has been revoked is a defective authorization.).

in reliance on the authorization.[11] 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.[12] In addition, revocation of an authorization would not prevent the continued use or disclosure of information by a non-covered entity that already received it pursuant to the authorization.

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 is free to 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 authorization. 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). However, this reminder is not 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.[13] 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.[14]

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. 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. Any process for revocation should not be unduly burdensome to

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

the individual such that it would create a barrier to or unreasonably delay the individual's exercising the right to revoke the authorization. For example, a covered entity cannot require all individuals to use a portal to submit a revocation if one or more individuals may not have easy access to the internet. In addition, if a covered entity provides a standard form for individuals to request revocation, the form should be readily available and accessible to the individual.

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.[15] The existence of a written revocation of authorization does not always mean that a covered entity has ''knowledge'' of the revocation, which would make the authorization defective.[16] Conversely, obtaining a copy of the written revocation is not required before a provider ''knows'' that an authorization has been revoked.[17]

To illustrate these points, consider a situation in which a person other than a covered entity obtains an individual's authorization, which it then presents to a covered entity, thus allowing the covered entity to disclose PHI. If the individual revokes the authorization by writing to that non-covered person who obtained the authorization, and neither the individual nor the other person informs the covered entity of the revocation, the 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 cannot require the non-covered researcher 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, if the individual does inform the covered entity of the revocation, even orally, the covered entity ''knows'' that the authorization has been revoked and can no longer treat the authorization as valid. Thus, in this example, 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).[18]

Finally, while a revocation must be in writing to apply the Privacy Rule requirement that a covered entity cease using and disclosing PHI pursuant to the authorization, a covered entity may cease using and disclosing PHI pursuant to an authorization based on an individual's oral request if it chooses to do so.[19]

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