



## Impact of the HIPAA Privacy Rule on Academic Research\*

---

*The Health Insurance Portability and Accountability Act of 1996 included provisions to protect the privacy of individually identifiable health information. To implement these privacy protections, the Department of Health and Human Services (HHS) issued a final Privacy Rule<sup>1</sup> on August 14, 2002, which must be implemented by April 14, 2003. The Rule will govern how health care providers use and disclose personally identifiable health information on their patients, including use and disclosure for research purposes. Even those researchers who might not qualify as “covered entities”<sup>2</sup> under the Rule may be affected if their research protocols require the use of individually identifiable health information obtained from a health care provider who is covered.<sup>3</sup>*

*The following is an overview of the key HIPAA Privacy Rule requirements related to clinical research.*

### USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR RESEARCH PURPOSES <sup>4</sup>

Before the Privacy Rule, protection of human subjects in research focused primarily on assuring that the research project was performed ethically and that the human subjects participated on the basis of informed consent. Federally sponsored research is generally subject to the requirements of the Common Rule. This is the set of standards common to federal agencies funding research involving human subjects. It attempts to minimize the risk to which the subjects are exposed and assures continuing oversight by Institutional Review Boards. While the Common Rule acknowledges the importance of confidentiality, it does not have extensive requirements regarding the matter. Likewise, the Food and Drug Administration (FDA) regulations governing clinical trials of new drugs and medical devices have some restrictions protecting the confidentiality of human subjects. The HIPAA Privacy Rule supplements both of these regulations; it does not replace them.

Effective April 14, 2003, a health care provider may only use or disclose protected health information (PHI) for treatment, payment and health care operations purposes. For all other purposes, including clinical research, the health care provider must obtain a written authorization from the individual, unless an exception

---

<sup>1</sup> See 45 C.F.R. Parts 160 and 164 for the HIPAA Privacy Rule provisions. While not covered in this paper, the Privacy Rule’s deferral to more stringent state law will be an important factor in the Rule’s implementation.

<sup>2</sup> 45 C.F.R. § 160.103. “*Covered entity* Means; (1) A health plan, (2) A health care clearinghouse, (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.”

<sup>3</sup> See important HHS comments about the Privacy Rule as it relates to research in the announcement of the final Rule in the Federal Register on August 14, 2002. See in particular 67 Fed. Reg. 53220 – 53239. While there is more about research elsewhere in the comments, most of the issues are discussed in these pages.

<sup>4</sup> See § 164.501 Definitions. “*Research* means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.” *Protected Health Information* (PHI) includes individually identifiable health information transmitted or maintained in any form or medium, including paper records.

applies. Although, historically, many clinical research organizations obtained “consents” to participate in research studies and, in some instances, general authorizations to use and disclose health information for purposes consistent with the research study, the Privacy Rule creates a distinct set of requirements for any document which purports to be a “valid” authorization. If the document does not have all of the key elements, the authorization is invalid and the health care provider may not disclose protected health information to the clinical researcher. A “valid” authorization must include six “core” components and three required statements and must meet two other implementation requirements.

## RESEARCH DISCLOSURES WITH AUTHORIZATION

### AUTHORIZATION “CORE” ELEMENTS

An authorization must have a specific and meaningful description of the information to be used or disclosed.<sup>5</sup> In the context of a clinical research study, the statement should describe in specific detail the types of information (e.g., laboratory results, x-rays) rather than a general statement such as “all health information related to your participation in the study.” Covered providers should be able to determine easily from the authorization what information is covered. Although an individual has the right to authorize the disclosure of his or her “entire medical record,” researchers should limit requests to that information necessary to carry out the applicable research protocol.

Second, an authorization must contain the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.<sup>6</sup> The purpose of this requirement is to assure that the provider who is permitted by the individual to disclose the information is clearly identified. For example, a physical therapist who receives an authorization directed to “all physicians” will not know with any reasonable certainty that the individual intended that the authorization apply to his or her records.

Third, an authorization must contain the name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.<sup>7</sup> The purpose of this requirement is to assure that the covered entity disclosing the information can reasonably identify the intended recipient. While this seems a relatively easy element to satisfy, it is unclear whether broad statements such as “to the clinical researcher and/or their representatives” would meet this requirement.

Fourth, an authorization must contain a description of each purpose of the requested use or disclosure. This can be easily satisfied by a brief introduction of the clinical research study, goals of the study, etc.

Fifth, an authorization generally must contain an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. Note, however, that for research purposes, the Privacy Rule provides that the statements “end of the research study” or “none” will satisfy the requirements for an expiration date or an expiration event.<sup>8</sup>

Lastly, an authorization must contain the signature of the individual and the date. If the authorization is signed by a personal representative of the individual, a description of such representative’s authority to act for the individual must also be provided.<sup>9</sup>

---

<sup>5</sup> 45 C.F.R. § 164.508(c)(1)(i).

<sup>6</sup> 45 C.F.R. § 164.508(c)(1)(ii).

<sup>7</sup> 45 C.F.R. § 164.508(c)(1)(iii).

<sup>8</sup> 45 C.F.R. § 164.508(c)(1)(v).

<sup>9</sup> 45 C.F.R. § 164.508(c)(1)(vi).

## AUTHORIZATION “REQUIRED” STATEMENTS

An authorization must also contain statements sufficient to notify the individual of the right to revoke the authorization in writing. Since the Rule provides for exceptions to the right to revoke, the authorization must describe those exceptions. As an alternative, the authorization can refer to such information that is already included in the covered entity’s Notice of Privacy Practices. A reference to the covered entity’s Notice of Privacy Practices will be sufficient.<sup>10</sup> In the clinical research context, covered entities (such as health care providers) may continue to use and disclose PHI obtained before the authorization was revoked, to the extent necessary to maintain the integrity of the research study. If a researcher has to account to the FDA for a subject’s withdrawal from a study, for example, the subject’s revocation of the authorization will not prevent the disclosure. Similarly, the information may be used in an investigation of scientific misconduct or to report adverse events.

The covered entity may not disclose PHI obtained after the effective date of the revocation. Only information “gathered” by the health care provider *before* the effective date of the revocation may be disclosed, but the rule does not define the term “gathered;” consequently, it is not clear whether laboratory and other clinical and diagnostic tests ordered before the revocation but not obtained by the provider until after the date of revocation may be disclosed to the researcher. A literal reading of the Rule suggests that only information in the possession of the provider on the date of a revocation may be disclosed to the researcher. Importantly, even where an individual revokes his or her authorization, the clinical researcher may continue to use the information previously received, as long as the use complies with the original authorization.

Authorizations generally must make clear that a covered entity is not permitted to condition the provision of treatment on the execution of a valid authorization.<sup>11</sup> The Rule makes an exception with regard to research involving treatment, however. HHS has recognized that if an individual desires to participate in a clinical research study and refuses to execute the authorization presented, the health care provider does not have to enroll the individual in the study. The individual cannot have it both ways; they cannot elect to participate, but refuse to share PHI with a clinical researcher.

An authorization must explain the potential for information to be re-disclosed by the recipient and that the recipient may not be required to comply with the Privacy Rule.<sup>12</sup> The covered entity obtaining an authorization for disclosure of information for research purposes does not have to include any statements about what the researcher will do to protect the privacy of the individual after receiving it from the entity and is not responsible for what the researcher does with the information. Notwithstanding this fact, HHS did note such information may be included voluntarily. Thus, researchers desiring to obtain PHI on patients might offer affirmative statements about their own policies or protocols to maintain the privacy and security of the information they receive.

## AUTHORIZATION IMPLEMENTATION REQUIREMENTS

Valid authorizations must meet two basic implementation requirements. The authorization must be written in plain language, and a copy of the authorization must be provided to the individual permitting the use or disclosure of their

---

<sup>10</sup> 45 C.F.R. § 164.508(c)(2).

<sup>11</sup> 45 C.F.R. § 164.508(c)(2)(ii).

<sup>12</sup> 45 C.F.R. § 164.508(c)(2)(iii).

PHI.<sup>13</sup> Again, while a relatively simple concept, surprisingly few providers offer patients copies of consents and similar documents they have signed.<sup>14</sup>

Although urged to do so by some of the persons submitting comments on the Privacy rule, HHS chose not to require that authorizations include statements about any remuneration the researcher may receive in connection with his or her research. Importantly, however, HHS has indicated that they plan on issuing “guidance” for the research community on financial conflicts of interest in the near future.

Lastly, HHS was asked by persons responding to HHS requests for comments to allow authorizations to include descriptions broad enough to cover future unspecified research, but they declined. HHS stated that the Privacy Rule does not provide for continued review of uses and disclosures like that carried out by an Institutional Review Board (IRB)<sup>15</sup> oversight of research for purposes of assuring compliance with the Common Rule. Without that oversight, HHS felt it was necessary to require an authorization of uses and disclosures for research purposes to be “study specific.” However, researchers may continue to use information obtained prior to April 14, 2003 pursuant to legal permissions, informed consents or IRB waivers that were not study specific.

## RESEARCH DISCLOSURES WITHOUT AUTHORIZATION

Although the general rule is that disclosures of PHI may not be made for research purposes without a written authorization, there are several exceptions related to IRB/Privacy Board Waivers, reviews preparatory to research, research on a decedent’s information,; public health disclosures, and use or disclosure of a “limited data set.”

### IRB/PRIVACY BOARD WAIVER TO AUTHORIZATION REQUIREMENTS

A covered entity is permitted to disclose PHI for research purposes without a written authorization if an IRB or Privacy Board has either waived the written authorization requirement or has approved a modified authorization. This applies to both government and privately funded research. The covered entity could use its own IRB or accept a waiver approved by some other IRB or, as an alternative, accept a waiver approved by a special Privacy Board.<sup>16</sup>

An IRB or a Privacy Board will have substantial responsibilities when considering approval of an alteration to or a waiver of an authorization. Documentation of such action must include a statement identifying the board and the date of approval and has to reflect proper consideration of the mandated criteria leading the board to conclude that the proposed disclosure poses no more than a minimal risk to the privacy of the individual. Certain elements must be present: (1) a plan to protect the identifiers<sup>17</sup> from improper use and disclosure, (2) a plan to destroy the identifiers

---

<sup>13</sup> 45 C.F.R. § 164.508(c)(3).

<sup>14</sup> 45 C.F.R. § 164.508(c)(4).

<sup>15</sup> As all clinical researchers know, Institutional Review Boards are required by federal regulations to oversee all federally funded research involving human subjects.

<sup>16</sup> Some universities are reporting that their Institutional Review Boards are not willing to take on the additional responsibility of reviewing and approving requests for waivers of the written authorization. See 45 C.F.R. § 164.512(i)(1)(i) regarding the role of an Institutional Review Board or a Privacy Board. A privacy board can be appointed to function much like an IRB with regard to the review of requests for waivers of the written authorization requirements for use and disclosure of PHI for research purposes. Their role is to assure that there is a legitimate and compelling reason for allowing access to health information without the patient’s consent.

<sup>17</sup> The word “identifiers” is the descriptor used in the Privacy Rule which refers to codes that could be traced back to the individual who is the subject of the protected health information.

as soon as possible, consistent with the purpose of the research, unless there is a compelling reason to retain the identifiers for health or research reasons or retention is required by law, and (3) adequate written assurances that PHI will not be reused or disclosed except where required by law, for research oversight, or for other research for which the use would be permitted.

To approve a waiver, an IRB or a privacy board has to find that disclosure poses a minimal risk to privacy and that the research could not practicably be done without the waiver and not without access to and use of the PHI. The documentation must describe the PHI for which access has been determined to be necessary and that the waiver has been approved, either under normal or expedited review procedures. IRB action must also be in compliance with the federal regulations governing IRBs. If a Privacy Board is used in lieu of an IRB, the Privacy Board's approval of a waiver of authorization requires a convened meeting of a majority of the board where a majority of those present vote for the approval.<sup>18</sup>

A privacy board's membership must be diverse and must include members who understand the effect of a research protocol on a research subject's privacy rights. Persons with conflicts of interest may not serve, and at least one member must be someone who is not affiliated with the covered entity or with a researcher or sponsor. This member also must not be someone "related" to any person who is affiliated with any of the involved entities.

Specifically, a Privacy Board which is authorized to grant waivers to the authorization requirements must (1) be composed of members with varying backgrounds and appropriate professional competency necessary to review the effect of the research protocol on the individual's privacy rights; (2) include at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and; (3) not have any member participating in a review of any project in which the member has a conflict of interest.<sup>19</sup>

## REVIEWS PREPARATORY TO RESEARCH

In recognition of the fact that it may be necessary for a researcher to review medical records before preparing a research protocol, the Rule permits a researcher to conduct this review without the patient's authorization. The researcher may not remove any of the information from the covered entity and the protected health information to which access is sought must be necessary for the research purposes.<sup>20</sup> HHS has made clear that this exception would preclude the electronic transfer of PHI from a covered entity to a researcher's office.

## RESEARCH ON DECEDENT'S INFORMATION

The Privacy Rule allows covered entities to disclose PHI of decedents to researchers for research purposes. However, the covered entity must obtain from the researcher (1) representations that the use or disclosure is being

---

<sup>18</sup> See 45 C.F.R. § 164.512(i)(2)(iv) for other details about the required privacy board procedures. This section also cites all of the relevant federal regulations governing Institutional Review Boards, since one of the Privacy Rule requirements is that the IRB make a statement that its approval has been done in compliance with its normal or expedited review procedures.

<sup>19</sup> 45 C.F.R. § 164.512(i).

<sup>20</sup> 45 C.F.R. § 164.512(i)(1)(ii) "Reviews preparatory to research. The covered entity obtains from the researcher representations that: (A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research; (B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and (C) The protected health information for which use or access is sought is necessary for the research purposes."

sought solely for research on the PHI of decedents; (2) documentation, at the request of the covered entity, of the death of such individuals; and (3) representations that the PHI is necessary for research purposes.<sup>21</sup>

Researchers should be aware of the fact that this is an area where state law could be more stringent than the Privacy Rule. If it is, state law will govern.

## PUBLIC HEALTH DISCLOSURES—FDA AND OTHER PUBLIC HEALTH AUTHORITIES

The Privacy Rule permits a covered entity to report information as necessary to ensure the public health, citing contagious diseases that may be indicative of bio-terrorism as an example. For example, covered entities are permitted to disclose PHI to a registry for research purposes, and those do not have to be government-sponsored registries. Academic and non-profit organization sponsored registries would qualify, provided the disclosure is required by law, is made pursuant to an IRB or privacy board waiver of authorization, is authorized by the individual, or consists only of a “limited data set.”

If the covered entity is disclosing information to a person<sup>22</sup> subject to the jurisdiction of the FDA with respect to an FDA-regulated product or activity, it may do so without authorization of the patient. Disclosure in these circumstances, however, is limited to purposes such as (1) adverse event reporting, (2) tracking of FDA-regulated products, (3) product recalls, repairs or replacement or for a “look back”,<sup>23</sup> or (4) to conduct post-marketing surveillance. This is not an exclusive list, so disclosures related to safety, quality or effectiveness of an FDA-regulated product would be a permissible disclosure, provided the disclosure is for a public health activity or purpose.

In reviewing comments on the proposed final Rule, HHS states that this exception would not permit disclosures of PHI to a drug or device manufacturer to evaluate the effectiveness of a marketing campaign. That is not considered a “public health” purpose. Importantly, whenever these public health disclosures are made without patient authorization, the covered entity must apply the “minimum necessary” standard.<sup>24</sup> In other words, they should release only that amount of information necessary to achieve the purpose. In their comments on the final Rule, HHS gives an example that relates to adverse drug reactions where it may be important to know what happened but not to whom it happened.

Adverse events can also be reported to a public health authority authorized to collect such reports or otherwise when required by law. For example, a federally-funded researcher employed by a covered entity could disclose PHI related to an adverse event to the NIH if required to do so by federal regulations.<sup>25</sup>

---

<sup>21</sup> 45 C.F.R. § 164.512(i)(1)(iii) Research on decedent’s information.

<sup>22</sup> See the August 14, 2002, HHS comments referring to the Food, Drug and Cosmetics Act definition of “person” which includes an individual, partnership, corporation, or association. (67 Fed. Reg. 53228). This includes drug and device manufacturers.

<sup>23</sup> “Look back” is related to blood and plasma products and the need to identify and quarantine blood and blood products that may be at risk of transmitting certain blood-borne diseases. This exception to the written authorization requirement would allow notification of people who have received possibly tainted products.

<sup>24</sup> § 164.502(b) describes the “minimum necessary” standard.

<sup>25</sup> See 67 Fed. Reg. 53229, HHS comments.

## DE-IDENTIFIED INFORMATION AND LIMITED DATA SET

The original Privacy Rule issued in December 2000 excluded from the definition of PHI information that had been “de-identified” in one of two ways. In one, a covered entity could use a qualified expert to apply scientific criteria to determine that the risk is very small that the information could be used to identify the individual, a fairly difficult standard to meet. The second method was to meet a “safe harbor” standard by stripping the health information of eighteen enumerated identifiers. The final Privacy Rule retains these options but does clarify that the re-identification code used in research studies is not an identifier that has to be removed.<sup>26</sup> It became clear that some research projects might need to release information back to the covered entity on a particular patient and there had to be some way to re-identify that patient. This way, the re-identification code can be disclosed with the de-identified information but the covered entity retains the key that would match the information with the patient. On the other hand, so-called keyed-hash message authentication code (HMAC) would not meet the standards as being a “re-identification” code. It is derived from individually identified information, and HHS has concluded that the key is shared with or provided by the recipient of the data in order for that recipient to be able to link information about the individual from multiple entities or over time.

Recognizing the limited value of de-identified information to clinical researchers, HHS created a new category of information called the “limited data set,”<sup>27</sup> which may be used or disclosed for research, public health, and health care operations purposes only. The “limited data set” requires the removal of fewer identifiers than is the case with de-identified information. The identifiers that would have to be removed focus on “facial identifiers.” These include photographs, names, medical record numbers, street address or postal address other than city, state and zip code, telephone and fax numbers, email address, social security number, certificate/license numbers, vehicle identifiers and serial numbers, URLs and IP addresses, account numbers, device identifiers and serial numbers, biometric identifiers, including finger and voice prints, or any other identifier by which an individual could be easily identified.

The recipient of a limited data set must sign a “data-use” agreement, a super-confidentiality agreement, which specifies that the information will be used only for the research, public health, or health care operations purpose for which it was received. The data-use agreement should require the researcher to use appropriate safeguards to prevent use or disclosure of the data other than as permitted by the Privacy Rule.<sup>28</sup> These assurances are similar to those required in “business associate agreements”.<sup>29</sup> Recipients who sign a data use agreement must agree not to re-identify the data or to contact the individual.

As with business associate agreements, there is no jurisdiction in HHS to enforce the data use agreements unless the recipient of the limited data set is also a covered entity. Generally, the disclosing covered entity is not liable for breaches of the data use agreement by the recipient, but the entity must take responsible steps to cure any breach or to end violations. There may be an obligation, however, to discontinue disclosure of PHI to the recipient and to report the recipient to HHS.

---

<sup>26</sup> See 45 C.F.R. § 164.514(b). Health information that is sufficiently stripped of its identifiers will not be considered individually identifiable and can be disclosed. It will not be considered protected health information. To meet this requirement, however, the information must not include name, geographic subdivisions smaller than a state, all dates related to an individual (except year), telephone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, recognizable photographs, and any other unique identifier.

<sup>27</sup> 45 C.F.R. § 164.514(e) sets out the this new category called “limited data set.”

<sup>28</sup> 45 C.F.R. § 164.514(e)(2).

<sup>29</sup> 45 C.F.R. § 160.103 defines “business associate,” and 45 C.F.R. § 164.504(e)(1) describes how business associate agreements are to be used.

Lastly, in applying the limited data set option, covered entities are expected to disclose the minimum amount of information necessary for the stated purpose. In other words, no more information should be released than is essential to the purpose. HHS clarifies that this could be accomplished by requiring the data requestor to specify the purposes of the limited data set and categories of data elements requested.

## ACCOUNTING FOR RESEARCH DISCLOSURES

Generally, the Privacy Rule requires that individuals have a right to receive an accounting of disclosures of PHI made by covered entities over a six (6) year period of time, with certain exceptions. Accountings must be provided, upon request, once a year without charge.

Fortunately, covered health care providers need not furnish an accounting of any disclosures pursuant to a valid authorization. Under this revised exception, covered entities are no longer responsible for providing an accounting for any disclosures authorized by the individual including disclosures made for research purposes. In addition, the covered entity does not need to include disclosures of PHI furnished in limited data sets to recipients under a data use agreement in any accounting of disclosures provided to the individual.

On the other hand, HHS declined to provide a blanket exception to the accounting requirement to authorizations issued under the IRB/Privacy Board waiver process.<sup>30</sup> They did agree, however, to permit a modified accounting procedure in certain instances. Specifically, covered entities may meet their accounting obligations if they provide individuals with a list of all protocols for which the patient's PHI may have been disclosed for research pursuant to a waiver of authorization (IRB or Privacy Board waiver), as well as the researcher's name and contact information. This procedure is available if the research disclosure involves 50 or more individuals.<sup>31</sup> The accounting must include the name of the study or protocol, a description of the purpose of the study and the type of PHI sought, and the timeframe of disclosures in response to the request. In addition, when requested by the individual, the covered entity must provide assistance in contacting those researchers to whom it is likely that the individual's PHI was actually disclosed.

The Rule does not appear to allow "aggregation" of research studies in order to meet the "50 individuals" test. Consequently, if a covered entity had disclosed PHI in two separate research studies pursuant to the waiver process and, in each study, only 30 records were disclosed, the simplified accounting procedures would not apply.

## HHS CLARIFICATIONS AND TRANSITION RULES

### RETROSPECTIVE RESEARCH STUDIES

The Privacy Rule permits the use or disclosure of PHI for retrospective research studies involving data re-analysis only where the researcher has obtained a valid written authorization or a waiver (IRB/Privacy Board). In other words, the mere fact that a study is characterized as "retrospective" does *not* change the general rules discussed above.<sup>32</sup>

---

<sup>30</sup> See 67 Fed. Reg. 53245 for a discussion of HHS's views about accounting for disclosures for research purposes. They recognize the added burden accounting imposes in large research projects.

<sup>31</sup> 45 C.F.R. § 164.528(b)(4).

<sup>32</sup> See 67 Fed. Reg. 53230.

## RESEARCH RECRUITMENT

HHS says that covered entities may continue to discuss with patients the option of enrolling in a clinical trial. This may be done without patient authorization and without an IRB or privacy board waiver. This permission does not extend, however, to disclosure of information to a third party for purposes of recruitment. In the latter instance, the covered entity either has to obtain an authorization from the individual or secure a waiver of that authorization as permitted by the Rule. HHS has recognized that the Privacy Rule certainly may alter some research recruitment because of this.<sup>33</sup> The belief is that the Privacy Rule will strengthen human subject privacy protections and research projects since neither the Common Rule nor the FDA's Human Subject Protection Regulations contain very much that addresses patient confidentiality. At least research subjects will now be granted the same privacy protections as anyone else on whom individually identifiable health information is maintained.

## TRANSITION PROVISIONS RELATED TO RESEARCH

The Privacy Rule allows covered entities to continue to use or disclose PHI created or received for a specific research study authorized before the April 14, 2003 compliance date. To do so, the provider must have obtained prior to the compliance date (1) an authorization or other express legal permission from an individual to use or disclose PHI for the study; (2) informed consent of the individual to participate in the research study; or (3) a waiver by an IRB of informed consent for the research study in accordance with the Common Rule or the FDA's human subject protection regulations.

In essence, this means that new authorizations for ongoing research studies will *not* have to be obtained after April 14, 2003. However, HHS clarifies that even if a researcher obtains an IRB waiver before April 14, 2003, an authorization would still be required if the researcher obtains informed consent at a later date. The revised Privacy Rule also eliminates distinctions in the application of these transition provisions based upon whether the research includes treatment and whether the research was conducted with an individual's legal permission or an IRB approved waiver. Note, however, HHS rejected the idea of creating a 'grandfather' clause that would have broadened the transition provisions by permitting covered entities to rely upon an express legal permission or informed consent that was not signed by the individual prior to the compliance date.<sup>34</sup>

## CONCLUSION

The HIPAA Privacy Rule will change the practices of health care providers in the use and disclosure of personally identifiable health information. Congress and HHS felt this was necessary to protect the privacy of patients whose health information is now routinely transmitted electronically. While the extent of the effect of these new restrictions on the use and disclosure of personally identifiable health information on clinical research activities is not yet fully known, it is clear that clinical researchers will need a working knowledge of the Privacy Rule. They need to understand how it will be applied to their research protocols, so that they may continue to have access to critical patient data.

---

<sup>33</sup> This could be particularly important to a university researcher who obtains PHI from a health care provider not part of the researcher's university.

<sup>34</sup> See 45 C.F.R. § 164.532(a) and (c). Helpful HHS comments appear in 67 Fed. Reg. 53248.