



**The Proposed HITECH HIPAA Rules:
Implications for the Research Community**

Executive Summary

On July 14, 2010, the HHS Office for Civil Rights (OCR) published proposed regulations to implement the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). *See* 75 Federal Register 40868. The proposed regulations portend substantial revisions to organization policies and practices, business associate agreements, and Notices of Privacy Practices. Some of these changes will also have a substantial impact on the conduct of research – some good, and some potentially bad.

OCR is seeking public comment on the proposed rules until September 13, 2010. We intend to develop comments on behalf of a consortium of organizations that are engaged in research. If you are interested in joining this consortium, please contact Kristen Rosati (krosati@csblaw.com; 602-381-5464).

This memo discusses a variety of proposed changes to the HIPAA Privacy Rule that will affect the conduct of research, including changes related to:

- A new rule prohibiting the “sale” of PHI;
- Authorizations for research; and
- Business associate agreements.

The memo identifies areas of concern with the proposed regulations, as well as additional areas where comments to OCR may streamline the research process.

I. Sale of PHI

The HIPAA Privacy Rule currently permits a covered entity to receive financial payment for a disclosure of PHI where that disclosure is permitted by the regulations (such as for research and quality assurance activities). Section 13405(d) of the HITECH Act (*codified at* 42 U.S.C. § 17935(d)) provides that “a covered entity or business associate shall not directly or indirectly receive remuneration in exchange for any [PHI] of an individual” unless the covered entity obtains the individual’s authorization.

To implement this requirement, OCR proposes to require a covered entity to obtain an authorization “for any disclosure of [PHI] for which the disclosure is in exchange for direct or indirect remuneration from or on behalf of the recipient of the [PHI].” *See* proposed 45 C.F.R. § 164.508(4). In the proposed rule, OCR also implements various statutory exceptions where

remuneration is permitted. *Id.* Four exceptions are particularly relevant to the research community:

- The prohibition against remuneration does not apply to disclosures of PHI for public health purposes under § 164.512(b) (the general rule on disclosures to public health authorities and for other public health purposes) or § 164.514(e) (disclosures of a Limited Data Set for public health activities). The HITECH Act requires HHS to evaluate whether payment under this exception should be capped at the cost to prepare and transmit PHI (as in the research exception); OCR seeks public comment on this issue. *See* 75 Fed. Reg. at 40891.
- The prohibition against remuneration does not apply to disclosures of PHI for research under § 164.512(i) (the general rule on research disclosures) or § 164.514(e) (disclosures of a Limited Data Set for research), “where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit the [PHI] for such purposes.” OCR requests public comment on the types of costs that should be permitted under this provision. *See* 75 Fed. Reg. at 40891.
- The prohibition against remuneration does not apply to disclosures “[t]o or by a business associate for activities that the business associate undertakes on behalf of a covered entity pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate for the performance of such activities.” OCR explains that, by referencing the business associate agreement requirements, it clarified that this exception covers disclosures for the business associate to perform activities on behalf of the covered entity. *See* 75 Fed. Reg. at 40891. “This proposed exception would exempt from the authorization requirement... a disclosure of [PHI] by a covered entity to a business associate or by a business associate to a third party on behalf of the covered entity, as long as any remuneration received by the business associate was for payment for the activities performed by the business associate pursuant to a business associate contract.” *Id.*
- OCR also proposes to add a general exception that was not in the statute, where the disclosure is permitted by the HIPAA Privacy Rule and the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI, or is a fee otherwise expressly permitted by other law. OCR explains that this would be limited to the “actual cost incurred to prepare, produce, or transmit” the PHI, unless a state or other law sets forth a specific fee for the type of disclosure. *See* 75 Fed. Reg. at 40892.

We urge comment by the research community on the following issues:

(1) The regulations should not prohibit indirect remuneration:

OCR’s interpretation that the statute prohibits indirect remuneration could pose a substantial problem for research, as well as collaborative quality assurance and other performance improvement activities. For example, many hospitals participate in research (or

quality improvement) collaborations, in which they contribute their PHI to a research database to create aggregated data sets, in exchange for the ability to utilize the aggregated information. Even if the hospital is not “paid” for its data contributed to the research database, the use of a research or QA tool *may* constitute indirect remuneration.

OCR should be encouraged to return to the remuneration standard required by the HITECH Act. The statute provides that a covered entity or business associates shall not “directly or indirectly receive remuneration in exchange” for PHI; in the statute, “direct or indirect” modifies the *receipt* of remuneration. In other words, under the statute, the covered entity could not receive payment directly or indirectly from a third party in exchange for disclosing PHI to the recipient.

In contrast, the proposed regulation prohibits “direct or indirect remuneration,” where “direct or indirect” modifies “*remuneration*,” and which thus could be interpreted as including a non-financial benefit. The intent of the statute clearly is to prohibit *financial* remuneration, as the title of the statute reflects the prohibition against the “sale” of PHI and all of the legislative history indicates a similar concern. *See* ARRA Conference Report, House Report No. 111-16 (Feb. 12, 2009) (explaining that section 13405 of the conference agreement was to require regulations to govern the “sale” of PHI); House Report No. 11-7(1) (Jan. 26, 2009) (explaining that the parallel section in the original House bill was to clarify that the “sale” of PHI would not be permitted); Senate Report 111-3 (Jan. 27, 2009) (same). The legislative history does not reflect any concern with the receipt of non-financial benefit. Moreover, the statutory exception for research demonstrates that only financial remuneration is contemplated, as it permits a “reasonable cost-based fee to cover the cost to prepare and transmit the [PHI].” OCR intended to follow the statutory language and intent. *See* 75 Fed. Reg. at 40891.

In commenting on this issue, we urge organizations to provide concrete examples of where they contribute data to research, and may receive some type of benefit in return. These examples will help demonstrate to OCR that there are many disclosures for research and quality assurance/performance improvement projects that work to improve the health of US citizens, as well as to improve the quality of the care provided, and should not be prohibited.

(2) The regulation should exclude Limited Data Sets from the prohibition on remuneration.

OCR proposes that the exception for research should apply to disclosures of a Limited Data Set (LDS) under 45 C.F.R. § 164.514(e). *See* 75 Fed. Reg. at 40891. (A LDS is mostly de-identified data, which may include dates related to an individual and geographic designations above street level. 45 C.F.R. § 164.514(e).) The inclusion of LDS was not required by the statute, and OCR explained that it added LDS to the regulation “to ensure that a covered entity or business associate that discloses [PHI] ...in limited data set form is also excepted from the authorization requirement. We believe it is consistent with the statutory language to also except the disclosure of a limited data set where Congress has already excepted the disclosure of fully identifiable [PHI] for the same purpose from the remuneration prohibition.” *See* 75 Fed. Reg. at 40891.

The research industry should urge OCR to exempt LDS from the provision entirely. The HIPAA Privacy Rule already limits the purposes for which a LDS may be disclosed to research, public health and health care operations. 45 C.F.R. § 164.514(e). More importantly, the Privacy Rule requires the recipient of a LDS to sign a Data Use Agreement, under which the recipient must agree to use the LDS only for the purpose permitted by the Data Use Agreement, to report to the covered entity any other use or disclosure of the LDS, not to use the LDS to identify individuals, and to require its agents to follow the same restrictions. *Id.* These provisions provide substantial protection against inappropriate use of the LDS, and we suggest comments to OCR to urge exclusion of LDS from the prohibition against receipt of remuneration.

If LDS is not excluded from the regulation entirely, we support the inclusion of the LDS in the research exception.

(3) Costs included in the cap on fees charged for PHI should contain a wide range of costs that permit organizations to recoup investment and other indirect costs.

The research exception permits remuneration “where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit the [PHI] for such purposes.” OCR requests public comment on the types of costs that should be permitted under this provision. *See* 75 Fed. Reg. at 40891.

We urge the research community to comment on the issue of what costs should be included in the cap. Specifically, many organizations have invested a substantial amount of money in the creation and maintenance of their clinical data repositories, in order to be able to capture, manage and adequately protect PHI used for research and quality assurance/performance improvement activities. In permitting others to utilize that data, those organizations should be permitted to recoup this investment and the costs of maintaining the data repositories. Organizations should also urge OCR to permit inclusion of the equipment costs and indirect costs associated with clinical data repositories and the research staff required to capture, manage and protect the data repositories.

(4) OCR should clarify the exception for disclosure of PHI to business associates.

OCR proposes an exception permitting disclosure of PHI “[t]o or by a business associate for activities that the business associate undertakes on behalf of a covered entity pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate for the performance of such activities.” *See* proposed 45 C.F.R. § 164.508(4). In other words, this would prevent a third party from paying a business associate for activities performed for the covered entity, in essence creating an indirect payment to the covered entity.

We urge comments to urge OCR to clarify that the regulation prohibits a business associate from receiving remuneration from a third party for activities on behalf of a covered entity, but does not prohibit a covered entity from receiving remuneration from the business associate (particularly if “remuneration” includes non-financial benefit, as discussed above). This appears to be OCR’s intent, as it states: “This proposed exception would exempt from the

authorization requirement... a disclosure of [PHI] by a covered entity to a business associate or by a business associate to a third party on behalf of the covered entity, *as long as any remuneration received by the business associate was for payment for the activities performed by the business associate pursuant to a business associate contract.*" See 75 Fed. Reg. at 40891 (emphasis added). Consistent with the explanation in the Preamble, OCR should clarify in the regulation that the remuneration at issue in this exception is the remuneration received by the business associate (not the covered entity). As with the research exception, if the concept of remuneration is broadly interpreted to include indirect remuneration (see comments above), the covered entity may be receiving a non-financial benefit from the disclosure of PHI to a business associate, such as access to a research or quality assurance tool.

II. Authorizations for Research

The HIPAA Privacy Rule currently poses two problems for research that involves storage of PHI (such as in biospecimen or data repositories). First, if a research participant is participating in a clinical trial and a research repository, the HIPAA authorizations for those activities must be separate.¹ This is because the HIPAA Privacy Rule permits a HIPAA covered entity to require an individual to sign a HIPAA authorization as a condition of receiving treatment in a clinical trial;² however, OCR has concluded that a covered entity may not condition treatment received in a clinical trial on signing a HIPAA authorization to include PHI in a research repository if that PHI will be used for purposes other than the specific clinical trial.³ The HIPAA problem is created because the current Privacy Rule prohibits combining authorizations for separate research activities into a "compound authorization," where the

¹ See HHS, *Research Repositories, Databases, and the HIPAA Privacy Rule* (NIH July 2004), available at http://privacyruleandresearch.nih.gov/pdf/research_repositories_final.pdf, at 6 ("May a single Authorization permit a covered entity to use or disclose PHI for multiple activities of a specific research study, including the collection and storage of tissues for only that study? Does the option for using a single Authorization differ if a research study also collects and stores PHI as part of a central repository for future research? A: A single Authorization may cover uses and disclosures of PHI for multiple activities of a specific research study, including the collection and storage of tissues for that study. In addition, where two different research studies are involved, such as where a research study collects information for the study itself, and collects and stores PHI in a central repository for future research, the Privacy Rule generally would permit them to be combined into a single, compound Authorization form. However, a compound Authorization is not allowed where the provision of research-related treatment, payment, or eligibility for benefits is conditioned on only one of the Authorizations, and not the other. See section 164.508(b)(3)(iii) of the Privacy Rule. For example, a covered entity that conducts an interventional clinical trial that also involves collecting tissues and associated PHI for storage in a central repository for future research would not be permitted to obtain a compound Authorization for both research purposes if research-related treatment is conditioned upon signing the Authorization for the clinical trial. Any compound Authorization must clearly specify the different research studies covered by the Authorization so the individual is adequately informed.").

² See 45 C.F.R. § 164.508(b)(4) (permitting a covered entity to condition participation in a clinical trial on signing an authorization to use or disclose the individual's PHI for the clinical trial).

³ See HHS, *Research Repositories*, at 6.

individual is required to sign one authorization but not the other.⁴ Having to separate these HIPAA authorizations often causes research participant (and researcher) confusion.

In the NPRM, OCR acknowledges that the research community has expressed concern about the lack of integration proposes to fix this prohibition against compound authorizations in research by amending § 164.508(b)(3) as follows:

An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization. *See* 75 Fed. Reg. at 40892-93.

This new requirement could be implemented through a variety of ways, including describing the “unconditioned research” (i.e. the repository) on a separate page of the authorization, by using a separate check-box for the unconditioned research, or distinct signature lines. OCR requests comments on “additional methods that would clearly differentiate to the individual the conditioned and unconditioned research activities on the compound authorization.” *Id.*

The second HIPAA authorization problem for research repositories is that OCR has interpreted the rule as requiring a HIPAA authorization to be study specific, because the rule

⁴ 45 C.F.R. § 164.508(b)(3) (“An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows: (i) An authorization for use or disclosure of protected health information for a research study may be combined with any other type of written permission *for the same research study*, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research.”) (emphasis added). *See also* 67 Fed. Reg. 53231, Aug. 14, 2002 (“Under the Common Rule, [OHRP] has interpreted the definition of “research” to include the development of a repository or database for future research purposes. *See also* <http://ohrp.osophs.HHS.gov/humansubjects/guidance/reposit.htm>. [HHS] interprets the definition of “research” in the Privacy Rule to be consistent with what is considered research under the Common Rule. Thus, the development of research repositories and databases for future research are considered research for the purposes of the Privacy Rule.”).

states that an authorization must describe each purpose of the requested use or disclosure.⁵ So, in the research repository context, an authorization may not seek permission to use or disclose PHI for future unspecified research, but may only seek permission to *store* PHI in the repository.⁶ This interpretation conflicts with the Common Rule, which permits an informed consent document to seek consent to use a subject's information in future research as long as the future research is described in enough detail to allow informed consent.⁷ This has caused a disconnect between the content of the informed consent document and HIPAA authorization form, again causing much confusion in the research industry.

The research community recognizes that this limitation should be changed. In its recent report regarding the HIPAA Privacy Rule and its impact on research, the Institute of Medicine recommended that HHS change its interpretation of this rule. See http://www.nap.edu/previewwidget.php?record_id=12458&wid=682312011320090608182255.

OCR recognizes this problem but has not yet proposed new language (or a new interpretation of the existing language). OCR solicits public comment on whether to modify its interpretation and is considering a number of options, including: (1) permitting an authorization to seek permission for future research, if adequately described; (2) permitting authorization for future research, with certain required elements or statements (and what those should be); or (3) permitting an authorization for future research, with limits on sensitive research areas, such as genetic or mental health research. See 75 Fed. Reg. at 40893-94. OCR will coordinate closely with the HHS Office for Human Research Protections and the Food and Drug Administration. *Id.* In fact, On July 15, OHRP posted a notice on its list serve encouraging comment on both the compound authorization and authorization for future research.

⁵ 45 C.F.R. § 164.508. See 67 Fed. Reg. at 53226 (Aug. 14, 2002).

⁶ See HHS, "Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule" (at http://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf). In this document at page 11, HHS states: "A valid Privacy Rule Authorization is an individual's signed permission that allows a covered entity to use or disclose the individual's PHI for the purposes, and to the recipient or recipients, as stated in the Authorization. When an Authorization is obtained for research purposes, *the Privacy Rule requires that it pertain only to a specific research study, not to nonspecific research or to future, unspecified projects. The Privacy Rule considers the creation and maintenance of a research repository or database as a specific research activity, but the subsequent use or disclosure by a covered entity of information from the database for a specific research study will require separate Authorization unless the PHI use or disclosure is permitted without Authorization (discussed later in this section). If an Authorization for research is obtained, the actual uses and disclosures made must be consistent with what is stated in the Authorization. The signed Authorization must be retained by the covered entity for 6 years from the date of creation or the date it was last in effect, whichever is later.*" (Emphasis added)

⁷ See 21 C.F.R. § 50.25; 45 C.F.R. § 46.116. See also *Institutional Review Boards and the HIPAA Privacy Rule* (HHS Aug. 15, 2003) at 11-12, at http://privacyruleandresearch.nih.gov/pdf/IRB_Factsheet.pdf.

III. Business Associate Agreements in Research

In its guidance on how the HIPAA Privacy Rule applies to research, HHS has explained that a business associate agreement between a covered entity and a third party in research is required where the third party performs de-identification services for the covered entity or creates a Limited Data Sets on behalf of the covered entity to use for research, because de-identification and the creation of a Limited Data Set is a health care operation under HIPAA.⁸ However, because research is itself not function or activity that is regulated under HIPAA (which is limited to the conduct of treatment, payment and health care operations functions), the disclosure of PHI for research, including research support services, does not require a business associate agreement.⁹ Many covered entities are not aware of this distinction, and

⁸ See HHS, *Clinical Research and the HIPAA Privacy Rule*, at http://privacyruleandresearch.nih.gov/pdf/clin_research.pdf (“Q: Does a covered entity need an individual’s Authorization before de-identifying the PHI or creating a limited data set? A: No. The Privacy Rule does not require a covered entity to obtain an individual’s Authorization before using or disclosing the PHI for creating de-identified health information or a limited data set. The Privacy Rule considers such activity to be a health care operation, as defined at section 164.501, of the covered entity. As such, a covered entity could contract with a business associate, including a researcher, to create de-identified data or a limited data set.”); (“Q: I am a researcher, and my research data source is asking me to sign a business associate agreement. Is this necessary? A: Business associates are persons who perform certain services for, or functions or activities on behalf of, the covered entity that require access to PHI, but who are not part of the workforce of the covered entity. If the data source is not a covered entity, no business associate contract is required because the Privacy Rule only applies to covered entities. If the data source is a covered entity, whether a business associate contract is required depends on the services, functions, or activities that the researcher is providing to, or performing for, the covered entity. *Researchers are not business associates solely by virtue of their own research activities (although they may become business associates in some other capacity, e.g., if de-identifying PHI on behalf of a covered entity)*. A business associate agreement will typically be a legally enforceable contract, so a researcher may wish to consult legal counsel before signing one.”) (emphasis added). See also HHS *Research Repositories* (“Q: Does the Privacy Rule permit a covered entity to de-identify health information or create a limited data set without obtaining Authorization, waiver of the Authorization requirement from an IRB or Privacy Board, or representations for reviews preparatory to research? A: Yes. In the Privacy Rule, creating de-identified health information or a limited data set is a health care operation of the covered entity, and thus, does not require the covered entity to obtain an individual’s Authorization, a waiver of the Authorization requirement, or representations for reviews preparatory to research. If a business associate is hired by a covered entity to de-identify health information or create a limited data set, such activity must be conducted in accordance with the business associate requirements at sections 164.502(e) and 164.504(e).”); (“Q: I am a researcher, and my research data source is asking me to sign a business associate agreement. Is this necessary? A: Business associates are persons who perform certain services for, or functions or activities on behalf of, the covered entity that require access to PHI, but who are not part of the workforce of the covered entity. If the data source is not a covered entity, no business associate contract is required because the Privacy Rule only applies to covered entities. If the data source is a covered entity, whether a business associate contract is required depends on the services, functions, or activities that the researcher is providing to or performing for the covered entity. *Researchers are not business associates solely by virtue of their own research activities (although they may become business associates in some other capacity, e.g., if de-identifying PHI on behalf of a covered entity)*. A business associate agreement will typically be a legally enforceable contract, so a researcher may wish to consult legal counsel before signing one.”).

⁹ See 45 C.F.R. § 160.103 (defining business associate: (“(1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this sub-chapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually

thus seek business associate agreements in the research arena. We suggest that OCR should take this opportunity to reflect this limitation in the definition of business associate.

In a related issue, we urge OCR to clarify that its incorporation of “data transmission services” as triggering a business associate agreement does not apply to research. Section 13408 of the HITECH Act (*codified at* 42 U.S.C. § 17938) provides that certain entities are business associates if they transmit PHI to a covered entity and require access to PHI on a routine basis, including Health Information Exchange Organizations, Regional Health Information Organizations, e-prescribing gateways, or vendors that contract with a covered entity to allow that covered entity to offer a personal health record to patients as part of its EHR. OCR implements this requirement by provided that a Health Information Organization (“HIO”), e-prescribing gateway or other person that provides “data transmission services” to covered entities are business associates if they transmit PHI to a covered entity and require access to that PHI on a routine basis. To the extent that a research partner transmits PHI to a covered entity (say, to a shared research repository housed by a covered entity), the language may be broad enough to include the exchange of PHI for research as “data transmission services.”

identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) *Any other function or activity regulated by this sub-chapter*; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this sub-chapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.).