

HHS Proposes Changes to HIPAA Privacy Regulation

Paul Smith, Reece Hirsch, Rebecca Williams, Clark Stanton, Keith Korenchuk, Richard Marks, Carol Pratt, Rebecca Reed, Rachel Glitz

Davis Wright Tremaine LLP
www.ehealthlaw.com

March 23, 2002

The Department of Health and Human Services has proposed major changes to the privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996. The proposed rule was published March 21, and affects the HIPAA privacy regulations due to go into effect in April of next year. DHHS is accepting comments on the proposed changes for 30 days.

Many of the changes contained in the proposed rule address problems identified by DHHS in its guidance on the Privacy Rule issued in July 2001 (http://www.dwt.com/practc/hc_ecom/bulletins/07-01_DHHS.htm). However, the proposed rule also contains a number of provisions that were not foreshadowed in the guidance that are likely to surprise, and please, many members of the healthcare industry.

The most profound change would be the elimination of the need for a written patient consent to allow providers to use protected health information for treatment, payment and operations. This consent is purely symbolic, because HIPAA effectively prevents anyone who refuses to give it from obtaining treatment.. The requirement results in a great deal of regulatory complexity, and threatens to impede access to health care. In its place, the amendment would require direct treatment providers to use best efforts to obtain a written acknowledgement of receipt of their notice of privacy practices.

The proposal would also give payers and providers greater latitude in sharing health information for payment and operations. Under the current rule a covered entity can use health information for its own purposes, but cannot, for example, give the information to another provider to use to obtain payment or for quality assurance. The proposed changes would permit the sharing of information for these and other similar purposes.

On the other hand, that most burdensome aspect of the current rule, the minimum necessary rule, emerges from the amendments largely unaltered, although in the preamble to the amendments DHHS repeats the assurances that it gave in last year's guidance that covered entities have flexibility to address their unique circumstances and can make their own assessment of what protected health information is reasonably necessary for particular purposes. The proposed rule would explicitly permit incidental disclosures resulting from such activities as discussions at nursing stations, the use of sign-in sheets, calling out names in waiting rooms, and the like.

Another significant modification in the proposed rule provides an extension period for covered entities to amend existing written contracts to include provisions that implement the current rule's business associate requirements.

A more detailed summary follows. If you would like to discuss these changes with a member of our HIPAA Practice Group, please visit our Web site at www.ehealthlaw.com for information on how to contact us.

Consent for Treatment, Payment and Health Care Operations

The most significant change in the proposed rule is the elimination of the requirement for providers to obtain an individual's written consent before using or disclosing protected health information for treatment, payment or operations. Under the proposed rule, covered entities would be permitted to obtain such a consent, but would not be required to do so. Covered entities that choose to obtain consent would have complete discretion in designing the consent process.

To balance the elimination of the consent requirement, the proposed rule would add a new requirement that health care providers with a direct treatment relationship must make a good faith effort to obtain an individual's written acknowledgment of receipt of the provider's notice of privacy practices. Other covered entities, such as health plans, would not be required to obtain this acknowledgment, but could choose to do so.

A direct treatment provider must attempt to obtain the acknowledgment at the time of first delivery of services, which is also the time when the notice of privacy practices must be given to the individual. However, in emergencies, the provider may delay provision of the notice until reasonably practicable and is not required to seek the acknowledgment.

The proposed rule does not specify the form of the acknowledgment, requiring only that it be in writing. DHHS comments that requiring an individual's signature on the notice itself is preferable, but that it would also be appropriate to have the individual initial a cover sheet of the notice. The proposed rule does not modify the content requirements for the notice of privacy practices.

Failure of a provider to obtain an acknowledgment would not be a violation of the privacy rule, so long as the provider has made a good faith effort and has documented its efforts and the reason for failure.

Disclosures to Another Entity for Payment and Operations

The current rule creates obstacles for providers and others who need to obtain protected health information from another covered entity for their own operational purposes. It is clear that a covered entity may disclose protected health information to a provider to enable the recipient to treat a patient. It is equally clear that a covered entity can disclose protected health information for its own operational purposes—for example, to obtain payment. However, the current rule precludes a covered entity from disclosing protected health information to another entity for the *recipient's* operational uses—for example, to obtain payment for itself, or to conduct quality assurance or peer review.

The proposed amendments would remedy this problem by allowing a covered entity to disclose protected health information to other covered entities, and to non-covered health care providers, to enable the recipient to make or obtain payment. The proposed rule would also allow a covered entity to disclose an individual's protected health information to another covered entity for limited operational purposes of the recipient, as long as the both entities have a relationship with the individual. This dispensation is, however, limited to disclosures for quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, case management, conducting training programs, accreditation, certification, licensing, credentialing activities, and health care fraud and abuse detection and compliance programs.

Finally, the amendments would clarify that covered entities participating in an organized health care arrangement may share protected health information for the health care operations of the OHCA.

Minimum Necessary Rule and Oral Communications

The minimum necessary rule has been one of the most controversial provisions of the privacy rule. It limits the use and disclosure of protected health information for payment or health care operations to the minimum necessary to accomplish the intended purpose. Covered entities must establish policies and procedures to identify people who need routine access to protected health information and the type of information they need, and to limit access accordingly. Requests that are not routine must be reviewed individually.

Covered entities have been concerned both by the administrative burden of implementing the new policies and procedures, and by the prospect that the rule will impede essential activities that result in incidental disclosures. In last year's guidance, DHHS stated that the minimum necessary rule was a reasonableness standard, and that covered entities have flexibility to address their unique circumstances

and can make their own assessments of what protected health information is reasonably necessary for particular purposes. DHHS repeats this statement in the commentary to the proposed rule, but is not proposing to change the language of the regulation.

As for oral communications, the advisory said that the rule required a common-sense approach, and was not intended to guarantee privacy against all risks. The proposed rule would make this explicit by allowing incidental uses and disclosures of protected health information that result from a use or disclosure that is otherwise permitted. Among the illustrations given of permissible disclosures are routine discussions about a patient at a nursing station that might be overheard by personnel not involved in the patient's care, the use of joint treatment areas, sign-in sheets, calling out names in waiting areas, and discussion of a patient during training rounds.

A covered entity must, however, reasonably safeguard protected health information to limit incidental disclosures. The amendment does not describe the kinds of safeguards a covered entity is expected to take to limit incidental disclosures. In last year's advisory, however, DHHS suggested asking waiting customers at pharmacies to stand back from the counter when another patient is being counseled; adding curtains or screens between patient treatment areas where oral communications are common; and installing cubicles, dividers and other shields in areas where multiple patient-staff communications occur routinely. The commentary to the proposed amendments emphasizes that erroneous or careless disclosures are not excused.

The proposed rule would make a few other minor changes to the minimum necessary rule, the most significant of which clarifies that the rule does not apply to uses or disclosures made under a specific authorization from the patient.

Business Associate Agreements

The privacy rule permits a covered entity to disclose protected health information to a business associate who performs a function or activity on behalf of the covered entity that involves the creation, use or disclosure of protected health information, so long as the covered entity enters into a contract with the business associate containing specific safeguards. DHHS noted that many commenters expressed concerns that the April 2003 compliance date of the current rule does not provide enough time for large covered entity organizations to reopen and renegotiate what could be hundreds of contracts affected by the business associate rules.

The proposed rule would allow covered entities to continue to operate under existing contracts with business associates for up to one year beyond the April 14, 2003 compliance date of the privacy rule. This transition period would be available to a covered entity if the covered entity has an existing contract or other written arrangement with a business associate and the contract is not renewed or modified between the effective date of the proposed rule and April 14, 2003. A covered entity's contract with a business associate would be deemed to be in compliance with the privacy rule until the sooner of (i) the date contract is renewed or modified after April 14, 2003 or (ii) April 14, 2004.

The transition period for business associate contracts does not apply to small health plan covered entities, which are not required to comply with the privacy rule until April 14, 2004. The transition period for entering into business associate contracts also would not apply to (i) oral contracts or other arrangements not reduced to writing and (ii) new written contracts entered into after April 14, 2003. The fact that an automatically renewing or "evergreen" contract becomes eligible for extension during the transition period would not require the covered entity to renegotiate the contract to include business associate provisions.

Covered entities would still be required to comply with HIPAA patient rights obligations commencing on April 14, 2003, even with respect to protected health information that is held by a business associate of the covered entity during the transition period. Covered entities would also be required to make protected health information available to the Secretary of DHHS as necessary for the Secretary to determine compliance, including protected health information held by a business associate.

An appendix to the proposed rule offers model business associate contract provisions to assist covered entities in meeting their compliance obligations under the business associate rules.

Use and Disclosure of protected health information for Marketing

The current rule defines “marketing” as a communication about a product or service, a purpose of which is to encourage recipients of the communication to purchase or use a product or service. A covered entity is generally not permitted to use or disclose protected health information for the purposes of marketing products or services that are not health-related without the express authorization of the individual.

The proposed rule attempts to simplify the current rule’s marketing rules by requiring covered entities to obtain an authorization from the individual before making *any* marketing communications. The proposed rule also would redefine what communications constitute marketing.

The proposed rule’s most significant change for marketing is the elimination of the current rule’s provisions that permit some marketing of health-related products and services without patient authorization. Instead, any marketing communication would require authorization by the individual.

The proposed rule clarifies the definition of “marketing,” to eliminate the implication that marketing is determined by the intent of the communication. Instead, the proposed rule makes clear that if the effect of the communication is to encourage recipients to purchase or use the product or service, the communication would constitute marketing.

The proposed rule clarifies the exception to the definition of “marketing” by specifying that communications for “case management” and “care coordination” do not constitute marketing, replacing the current rule’s exception for communications made “in the course of managing the treatment of [the] individual,” which was deemed to be less clear.

The proposed rule would also eliminate the distinction in the definition of “marketing” relating to written communications for which a covered entity is compensated by a third party. Unlike the current rule, the proposed rule would exclude communications from the definition of marketing even if the covered entity receives remuneration from a third party for making them. DHHS noted in the preamble to the proposed rule that the intent of this change is to ensure that the covered entity is not required to obtain authorization for certain treatment-related communications, such as prescription refill reminders, where the covered entity may receive compensation from a third party.

If an authorization is required for a marketing communication, the proposed rule would require that authorization contain a statement that the marketing is expected to result in direct or indirect remuneration to the covered entity from a third party, if applicable.

Parents as Personal Representatives of Minors

The privacy rule generally gives control of a minor’s health information to the parent, guardian, or person acting *in loco parentis*. This is not the case, however, where state law or a court allows the minor, or someone other than the parent, to consent to treatment—in these cases the minor or other person giving the consent controls the health information. The privacy rule also permits the exclusion of the parent where the parent consents to a confidential relationship between the minor and a physician or where the covered entity determines that disclosure to the parent would be harmful to the minor.

The proposed rule would continue to defer to state law by clarifying that HIPAA does not overturn state laws that give providers discretion to disclose health information to parents, or that prohibit the disclosure of health information to a parent. The amendments would also permit disclosure to a parent who is not the personal representative of a child where state law permits the disclosure.

Use and Disclosure for Research

The proposed changes do not alter the basic rule that protected health information may not be used or disclosed for research without either a written authorization or a waiver of authorization approved by an Institutional Review Board or a Privacy Board. However, DHHS is proposing changes that significantly simplify the administrative burdens for obtaining authorizations and assessing requests for waivers of authorization.

Under the proposed regulations, authorizations for *any* purpose, including research, must include the same required elements. DHHS's proposed standardization of authorization requirements will eliminate three sets of research-specific requirements which, in the current rule, must be added to the core elements when a covered entity wants to use or disclose its own (existing) protected health information for clinical trials, or to disclose protected health information to another covered entity for treatment, payment or operations.

In response to concerns about how to specify an expiration date or event in a research study, DHHS proposes to permit the use of "end of the research study" or the equivalent on authorizations to use or disclose protected health information for research. Respecting the need and value of medical databases, DHHS also proposes to allow "none" or the equivalent to be used when protected health information will be used or disclosed solely to create or maintain a research database or repository. However, DHHS clarifies in the preamble that subsequent research using information maintained in the database would require an authorization with a specified expiration date/event or until the "end of the research study."

Another proposed simplification involves standardizing the rules on compound authorizations. The proposed regulations would allow authorization for a specific research study to be combined with an informed consent form for all types of research, not just research that includes treatment. However, a distinction that is retained explicitly in the proposed regulations is the permissibility of conditioning the provision of care on an authorization in research that includes treatment only.

DHHS also proposes significant changes to the criteria for authorization waivers in an effort to more closely resemble the Common Rule's waiver of informed consent and to reduce internal redundancy and inconsistencies. Of the current eight criteria for authorization waivers, DHHS is proposing to keep just three: (1) the use and disclosure of protected health information involves not more than minimal risk, (2) the research could not practicably be conducted without the waiver or alteration of authorization, and (3) the research cannot practicably be conducted without access to and use of the protected health information. Whether there is an adequate plan to protect identifiers from improper use and disclosure or to destroy identifiers at the earliest possible time and whether there are adequate assurances against reuse or redisclosure would be downgraded from criteria to factors for the IRB or Privacy Board to consider in its minimal risk analysis.

Finally, DHHS proposes changes to the transition provisions to remove distinctions between research that does or does not include treatment. Under the proposed regulations, for both categories of research, protected health information for a specific research study that started before HIPAA's compliance deadline could be used or disclosed without an authorization, provided the covered entity obtained either an IRB-approved informed consent or waiver of informed consent or any other legal permission to use or disclose protected health information before April 14, 2003. HIPAA's transition provision applies to information that is created or received before *or after* the compliance deadline as long as it is part of the same research study.

Use and Disclosure Requiring Authorization

DHHS has proposed a number of changes involving authorizations for the use or disclosure of protected health information. One change would standardize the core provisions in authorization forms, including authorizations for research involving treatment. This would simplify the forms and reduce the need to maintain different forms depending upon the circumstances under which the authorization is obtained. As an example, all authorization forms could include a description of the purpose of the use or disclosure,

but this information does not have to be provided when the disclosure is initiated by the individual who is the subject of the protected health information. DHHS has also proposed a number of changes to ease the authorization requirements where protected health information is sought for use in research studies.

De-Identification of protected health information

Under the current rule a covered entity may freely use and disclose protected health information if the information is "de-identified." To de-identify, a covered entity may rely on "a person with appropriate knowledge and experience" using generally acceptable statistical and scientific principles and methods. The rule also has a safe harbor which allows a covered entity to treat information as de-identified if it removes all unique identifiers, including 18 specified identifiers, and it has no actual knowledge that the remaining information could be used to identify an individual. The proposed rule does not modify either method of de-identification. Rather, DHHS has requested comment on an alternative approach, which would permit covered entities to use and disclose a limited data set for research, public health and health care operations only. The limited data set would exclude readily identifiable information, such as name, street address, telephone and fax numbers, e-mail address, social security number, certificate/license number, vehicle identifiers and serial numbers, URLs and IP addresses, and full face photos. However, the data could include information on admission, discharge and service dates, the date of death, age (including age 90 or over) and five-digit zip code. Disclosure of a limited data set would be conditioned upon a covered entity's obtaining an agreement from the recipient, limiting the recipient's use to the purposes specified in the privacy rule, limiting who may use or receive data, and agreeing not to re-identify the data or contact the individuals.

In addition to DHHS's limited data set proposal, the Department clarifies that the privacy rule does not prohibit the age of an individual from being expressed as an age in months, days or hours (and has solicited comment on whether date of birth is needed for the purposes of the limited data set).

Disclosures of Enrollment and Disenrollment by Group Health Plans

The proposed rule makes clear that group health plans are permitted to share enrollment and disenrollment information with plan sponsors without amending plan documents. This policy regarding disclosures of enrollment or disenrollment information was addressed only in the preamble to the current rule and not explicitly in the regulation itself. To make the policy clear, the NPRM adds an explicit exception to clarify that group health plans (or health insurance issuers or HMOs, as appropriate) are permitted to disclose enrollment or disenrollment information to a plan sponsor without meeting the plan document amendment and other related requirements.