AHA
Advancing Health in America

HOSPITAL HIGHLIGHTS

Prepared for AHA members whenever there is important HIPAA-related news.

FINAL HIPAA PRIVACY RULE CHANGES

August 12, 2002

On August 9 the Department of Health and Human Services (HHS) released final regulations implementing changes to the HIPAA Privacy Rule. The final regulations will be published in the *Federal Register* August 14, and will be effective October 14, 2002. Hospitals must comply with the privacy rule, including the changes set forth in the final regulations, by April 14, 2003. HHS said that it intends to update its previous guidance and provide further guidance in the form of frequently asked questions and other materials to help covered entities comply with the rule.

Please find attached to this document a fax-back form you can fill out to sign up for an AHA conference call to discuss the final rule. This Hospital Highlights also is available on our Web site by clicking on "HIPAA" at www.aha.org.

AHA is extremely pleased that the final regulations, consistent with AHA's comments to HHS, adopt almost all of the changes proposed in the notice of proposed rulemaking (NPRM) published March 27, 2002. In doing so, the final regulations retain strong protections for patients' medical privacy rights while eliminating some major barriers to timely and effective care.

Most importantly, the final regulations adopt the proposals to:

- allow written acknowledgment to substitute for redundant written consent requirements;
- retain written consent as an option;
- allow the disclosure of "facially de-identified" data for health care operations and research pursuant to a data use agreement;
- allow an additional year to incorporate the business associate requirements into existing written agreements that are not up for renewal; and
- significantly simplify the research authorization requirements and criteria for waiver of authorization.

In addition, HHS addresses several issues identified in AHA's comments to clarify that certain permissible disclosures and incidental disclosures do not create business

associate relationships, that hospital newsletters are not prohibited marketing, to limit the impact of the delayed security rule on arrangements and safeguards for implementing the privacy regulation, and to make it feasible to implement the minimum necessary requirement.

WRITTEN ACKNOWLEDGMENT

As an alternative to the consent requirement, the final regulations require hospitals and other providers with direct treatment relationships to make a good faith effort to document, in writing, the patient's receipt of their notice of privacy practices. The precise method is left to each covered entity, and may be done, for example, by having the patient sign an acknowledgment list or a cover sheet attached to the notice. No written acknowledgement is required in emergency situations. HHS also encourages, but does not require, the use of a "layered notice." A layered notice consists of a short summary of the patient's rights and other important information *and* the full notice required by the HIPAA privacy rule layered beneath the summary. The layered notice does *not* alleviate the requirement that hospitals provide individuals with a notice of privacy practices meeting the requirements of the privacy rule, but allows hospitals also to provide patients with a short summary that can be more patient-friendly.

CONSENT

The final regulations retain written consent as an option for providers with a direct treatment relationship with the patient. Such providers are not required to, but may, obtain individual consent to use or disclose protected health information for treatment, payment and health care operations. In addition, the final rule adopts the proposal to allow providers to disclose protected health information for the treatment activities of another provider, the payment activities of another provider or covered entity, and certain limited health care operations (*e.g.*, quality assurance, accreditation, fraud and abuse audits) of another covered entity that has or had a relationship with the subject of the information.

LIMITED DATA SET

HHS adopts the proposal advocated by AHA to allow covered entities to disclose, pursuant to a data use agreement, "facially de-identified" information for health care operations, public health and research activities. This limited data set may include zip codes, date of birth and dates of service. It may not include patient identifiers, postal address, medical record numbers and the like. The final regulations set forth the requirements for a valid data use agreement. The final regulations also permit a covered entity to disclose protected health information to its business associate for purposes of creating a limited data set. Thus, under the final regulations, hospitals may disclose information to their state and metropolitan hospital associations for health care operations or permit the association to create the limited data set, pursuant to a business associate agreement, and use such data set for health care operations. In response to AHA's comments, HHS clarifies that multiple hospitals may enter into one data use agreement with a state and metropolitan hospital association and that a single agreement can contain the business associate and data use provisions.

INCIDENTAL DISCLOSURES

As AHA requested, HHS adopts the proposal to add new provisions for "incidental disclosures," defined as disclosures that are limited in nature and occur as a byproduct of an otherwise permissible use or disclosure. Incidental disclosures will not be considered a violation of the privacy rule if reasonable safeguards are in place and the minimum necessary requirements are met. Therefore, if a person in the waiting room overhears a discussion between a doctor and a nurse, or if a visitor sees an X-ray on a light board, the disclosure is considered an incidental disclosure and not a violation, if the requirements stated above are met. In the preamble to the final regulations, HHS clarifies that incidental disclosures are not just those associated with a treatment activity and are not limited to communications between providers and medical staff. For example, if a physician discusses a billing matter with a member of the hospital's administrative staff and a person in the waiting room overhears, such disclosure is an incidental disclosure if the requisite safeguards and minimum necessary standards are in place. HHS clarifies further that the minimum necessary requirements are "intended to be consistent with, and not override, professional judgment and standards."

DE-IDENTIFICATION

In the final regulations, HHS adopts its proposed clarification that information about a person's age may be described in terms of months, days or hours and still qualify for the de-identification safe harbor. The regulations also implement the proposed change to the de-identification safe harbor criteria to allow unique codes that meet certain requirements in the privacy rule. However, HHS also clarifies that case codes created with a "hashing" system that uses social security numbers or other fields listed in the regulation cannot be included in data that meet the de-identification safe harbor.

BUSINESS ASSOCIATES

The final regulations adopt the NPRM's proposal to allow covered entities an additional year to amend existing written agreements to incorporate business associate provisions. Agreements that come up for renewal, other than through an automatic renewal without negotiation, must be modified to incorporate the business associate provisions at that time. All other agreements must be modified by April 14, 2004, but HHS makes clear that hospitals still must comply by April 14, 2003 with the individual rights requirements with regard to information held by their business associates.

In addition, in response to AHA's comments, HHS clarifies that third parties who perform a service or function for a hospital and may inadvertently come into contact with protected health information are not business associates (*e.g.*, janitors). HHS also clarifies that participants in an organized health care arrangement ("OHCA") do not need a business associate agreement with each other to the extent that the disclosure of protected health information *relates to the joint activities of the OHCA*. HHS also clarifies that a covered entity does not need a business associate agreement with a researcher, whether the researcher is performing its own research or research on behalf of the covered entity.

HHS declines to provide a business associate certification process or to eliminate the requirement for a business associate agreement between two covered entities where the relationship otherwise meets the definition of "business associate."

Regarding liability for business associate activities, HHS provides some guidance regarding when a covered entity is considered to have knowledge of a violation by its business associate, stating that the determination is based on "common principles of law that dictate when knowledge can be attributed to a corporate entity." Finally, HHS addresses many of AHA's concerns about the proposed sample business associate agreement by revising it to conform more closely to the requirements of the privacy rule. The agreement, however, continues to include some optional provisions that hospitals may not want to include in their business associate agreements.

MARKETING

The final regulations adopt the marketing proposals from the NPRM, specifically prohibiting the use or disclosure of protected health information for marketing activities without individual authorization. The final regulations also state that without each individual's authorization, a covered entity is prohibited from disclosing protected health information to a third party for the marketing of the third party's products or services. Certain treatment and case and disease management activities are not considered marketing. In addition, in response to AHA's comments and requests for clarification, the final regulations make clear that hospital newsletters and other communications regarding a hospital's own health-related products or services or for general health promotion purposes are not marketing, so long as the communication or newsletter does not promote a particular product or service of a third party. Therefore, for example, a hospital can send out newsletters about lowering cholesterol, the latest in diabetes treatments, its new maternity center or health classes and programs it offers. The issue of remuneration from a third party, whether direct or indirect, is not a criterion that is considered in deciding whether an activity is marketing. There were no changes to the fundraising requirements.

STRUCTURAL OPTIONS

The regulations finalize the proposal to allow any covered entity to designate itself a hybrid entity and, thereby, separate its health care component (which must comply with the privacy rule) from its non-health care component (which is not subject to the requirements of the privacy rule). A hybrid entity may include in its health care component only the entity's covered functions and the parts of the entity that perform business associate-type functions for the health care component. Therefore, hospitals may choose to segregate certain of their functions or components from their plan for HIPAA compliance, provided that protected health information is not disclosed to these components in a way not otherwise permitted by the privacy rule. In-house legal counsel also can be included in a hospital's health care component, but only with regard to services for the health care component involving protected health information. HHS clarifies that a business associate agreement still is required between covered entities and their outside legal counsel, if such counsel will receive protected health information in the course of their services.

The final regulations also adopt the exemption for employment records received by entities in their capacity as an employer. HHS clarifies that health information a hospital receives about an employee in its capacity as a provider is protected health information subject to the privacy rule. If such information is then released to the hospital's human resources department pursuant to patient authorization, for example, for purposes of obtaining a medical leave of absence, the information in the human resources department would not be considered protected health information. Thus, health information a hospital receives in its capacity as an employer is not subject to the HIPAA requirements.

ACCOUNTING OF DISCLOSURES

HHS adopts the proposal in the NPRM to exempt from the accounting of disclosures requirements disclosures made pursuant to individual authorization. In addition, such disclosures are not subject to the minimum necessary requirements. The final regulations also exempt incidental disclosures and disclosures of limited data sets from the accounting of disclosures requirements.

With respect to disclosures of data for research under a waiver of authorization by an internal review board or privacy board, HHS provides an alternative: each patient's record can be annotated with the information required for an accounting, or every patient who requests an accounting can be given a list of protocols (and related information) about all of the disclosures for research under a waiver of authorization during the time period. Curiously, HHS also requires the covered entity to assist the patient in contacting the researcher if it is "reasonably likely" that the patient's information was included in the data provided. This requirement could be confusing to patients because the waiver criteria make it extremely unlikely that researchers who receive information under such a waiver will receive or retain any information that would make it feasible to determine whether the researcher received information pertaining to the patient.

SECURITY

In the preamble to the final regulations, HHS clarifies that the requirements of the security regulations (which have not yet been finalized) will apply only to electronic health information systems. In contrast, the safeguard requirements that hospitals need to implement under the privacy rule cover all protected health information, in whatever form or medium. Thus, HHS states that the majority of safeguards hospitals will implement under the privacy rule will not be affected by the final security regulations, once published.

RESEARCH

HHS adopts the proposals from the NPRM that significantly simplify the requirements for research authorizations and the criteria for waivers of authorization. The final regulations also make clear that covered entities may rely on an internal review board or privacy board determination regarding the minimum necessary information for the research. In the preamble to the regulations, HHS makes clear that it intends to "strictly enforce" the requirements for obtaining individual authorizations for purposes required by the privacy rule, including authorizations for a specific research project. Indeed, HHS says that the common practice of obtaining

patient authorization to use data for future unspecified research is not permissible under the regulation. However, a patient can provide authorization for information to be included in a research database or registry.

The final regulations also permit the use of a limited data set, pursuant to a data use agreement, for research purposes (as discussed above). In fact, the preamble states that an internal review board of an entity with an assurance of compliance with the research regulations may have policies under which disclosures of limited data sets for research purposes do not require internal review board review.

Finally, HHS clarifies that communications to an individual regarding participation in a clinical trial are not considered marketing and may be made by the covered entity without individual authorization or an internal review board or privacy board waiver of authorization. However, if a third party will contact the prospective participant, authorization of the individual or waiver of authorization by an internal review board or privacy board is required.

AHA
Advancing Health in America

AHA Member Conference Call
Final Changes to the HIPAA Medical Privacy Rule

FAX BACK FORM

Yes, I will participate in the member conference call on the final changes to the HIPAA Medical Privacy Rule.

My preference for the time of the conference call is (check most preferred time):

_____Tuesday, August 27 at 3 p.m. EDT (2 p.m. CDT, 1 p.m. MDT, 12 p.m. PDT)

_____Thursday, September 5 at 3 p.m. EDT (2 p.m. CDT, 1 p.m. MDT, 12 p.m. PDT)

_____Thursday, September 12 at 3 p.m. EDT (2 p.m. CDT, 1 p.m. MDT, 12 p.m. PDT)

Print Clearly

Name_____Title_____

Organization _____

City _____State_____

Phone_____Fax_____

E-mail _____

Please fax back by noon on Wednesday, August 21
to Shawna Brown at 1-312-422-4590 (Fax)

For more information about the proposed changes to the HIPAA medical privacy rules, contact Lawrence Hughes, Director, Member Relations at 312-422-3328.