focus on

Medical Privacy

June 2001

HIPAA and the Federal Privacy Standards for Health Information

Overview

On December 28, 2001, the Department of Health and Human Services ("HHS") published the long-awaited final privacy rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The rule became effective on April 14, 2001 and most covered entities have only two years to come into full compliance with this sweeping and complex set of new legal requirements.

The regulations will have a substantial impact on virtually every sector of the health care industry. They will affect the use and disclosure of protected health information by health care providers, health plans, health care clearinghouses, employers, and companies that provide services to those involved in the delivery of health-related services. In general, the rule requires covered health care providers to obtain patient consent before using or disclosing the protected health information of any individual for treatment, payment or certain "health care operations."[1] Health care providers that do not have a direct treatment relationship with the patient (e.g., laboratories, physicians called for a consultation) and health plans may use or disclose protected health information for treatment, payment, and health care operations, provided that the provider or health plan has included these activities in the "Notice" of information practices that it has published and distributed to patients and enrollees. Except for a few activities that are listed in the regulation, such as public health reporting, no other use or disclosure may be made without specific patient authorization.[2]

1. 45 C.F.R. 164.506(a).
2. 45 C.F.R. 164.502.

Modifications to the rule

Secretary Thompson stated that some concerns about the rule would be addressed through guidelines and recommended modifications. Under the law, during the first 12 months after which a standard is initially adopted (i.e., between April 2001 and April 2002), HHS is permitted to adopt modifications only if the Secretary determines that such modifications are necessary in order to permit compliance with the standard. The Secretary stated that the Department "will make it clear" that "doctors and hospitals will have access to necessary medical information about a patient they are treating" and that patient care will not be burdened "by the confusing requirements surrounding consent forms."

Covered entities

The HIPAA statute lists three types of covered entities: health plans, health care clearinghouses and certain health care providers. The regulation introduces three additional subcategories of covered entities - affiliated entities, hybrid entities and "organized health care arrangements" - that are intended to help facilitate compliance among related participants in the health care delivery and payment process. First, covered entities that are legally separate entities but subject to common ownership and control may designate themselves as a single covered entity for purposes of complying with the requirements of the rule ("affiliated covered entities"). Second, the rule applies to those persons or organizations that meet the definition of "covered entity" because they perform what the rule defines as "covered functions," but whose covered functions are not their primary purpose ("hybrid entities"). For hybrid entities, only the subsidiary or subdivision that performs covered functions ("health care component") is subject to the requirements of the rule. Lastly, the final rule permits joint compliance by covered entities that function as a single, integrated health care delivery system or care setting in which the participating covered entities hold themselves out to the public as operating jointly ("organized health care arrangement").

Protected health information

The requirements of the rule apply to "protected health information," which means health information created or received by a health care provider, health plan, employer, or health care clearinghouse which relates to a person's past present or future physical or mental health or condition, to the provision of health care to that person, or the past present or future payment for that person's health care. Information that meets these specifications and is transmitted or maintained by a covered entity in any form constitutes protected health information. This definition effectively makes all health information - paper, electronic and oral - subject to the requirements of the rule. Information that has been de-identified in accordance with the rule is not considered protected health information.

Patient consent

For health care providers that have a direct relationship with the patient (e.g., doctors and hospitals), the rule requires that they obtain specific "consent" of the patient for uses and disclosures of protected health information for purposes of treatment, payment or health care operations, except in emergencies and in situations where the provider is obligated by law to provide care.[3] The final rule does permit health care providers to condition treatment on the

3. There is an exception from the consent requirement for providers that have an "indirect treatment relationship" to the patient, a group that includes physicians that consult on a case, as well as labs and pharmacies and others that provide health care on the order of another health care provider. The "regulatory authorization" to use and disclose information for treatment, payment and health care operations remains in place for health plans and clearinghouses. § 164.502(a)(1)(iii). Uses and disclosures by covered entities is subject to the requirements or limitations in any business associate contracts they have with the other covered entities from whom they obtain information, and to the uses and disclosures that they have disclosed to the public in their "notice," discussed below.

provision by the patient of the required consent. Other covered entities - health plans and clearinghouses - may obtain specific patient consent for purposes of treatment, payment or operations but are not required to do so. Health care providers also may obtain a joint consent on behalf of other covered entities. In the event that a health care provider or other covered entity has obtained a consent that conflicts with any other authorization or consent received by the entity, the entity may only use or disclose protected health information in accordance with the terms of the most restrictive valid consent.

Patient authorization

For virtually all uses or disclosures of protected health information that do not involve treatment, payment or health care operations, the rule requires that covered entities obtain a valid patient "authorization." The final rule prohibits covered entities from conditioning the provision to an individual of treatment, payment, enrollment in a health plan or eligibility for benefits on the provision of an authorization, except under certain specified circumstances (such as clinical research). Patients are permitted to revoke their authorization at any time except to the extent that the covered entity has taken steps in reasonable reliance on the otherwise valid authorization. In certain limited circumstances, a covered entity may use or disclose protected health information without patient authorization provided that the patient has advance notice and is given an opportunity to agree to or to object to the proposed use or disclosure. Such notice and patient agreement or objection to the proposed use or disclosure may be made orally.

Required notice

Individuals have the right to receive adequate notice of a covered entity's policies and practices governing its use and disclosure of protected health information and of their rights with respect to that information. The notice must be in plain language and include a description of the types of uses and disclosures that the covered entity is permitted to make for treatment, payment, and health care operations, including at least one example. Covered entities that intend to contact individuals to inform them of health-related benefits and services or fundraise are required to make special disclosures in a separate statement. Special notice requirements apply to group health plans making disclosures to the plan sponsor. The final rule also includes specific requirements regarding electronic notice, as well as joint notice by separate covered entities that participate in organized health care arrangements.

Business associates

The rule requires covered entities to impose certain contractual requirements and obtain certain privacy assurances from "business associates" that receive or create protected health information from or on behalf of the covered entity. The final rule, however, eliminated the requirement that individual patients be considered third-party beneficiaries of the contract between the covered entity and the business associate. If a covered entity knows of a material violation of the contract by a business associate, the covered entity is required to take reasonable steps to cure the breach or terminate the contract. A covered entity may permit a business associate to use protected health information for its own management or administration purposes and may permit the business associate to disclose protected health information under certain circumstances. Covered entities may authorize their business associates to combine protected health information from more than one covered entity to permit data analyses that relate to the health care operations of the respective covered entities ("data aggregation"). Health care clearinghouses that function as the business associate of other covered entities have special requirements.

Minimum necessary disclosures

With the exception of disclosures by a provider to another provider for treatment purposes, the rule requires that covered entities use or disclose only the minimum amount of protected health information that is necessary to achieve the purpose of the use or disclosure. The final rule, however, significantly clarified this requirement by detailing the administrative procedures that covered entities must have in place to implement the minimum necessary standard. For example, for disclosures that it makes on a routine basis, a covered entity need not make individualized determinations, but instead may implement policies and procedures that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, covered entities must develop criteria designed to limit the amount protected health information disclosed, and review requests for disclosure on an individual basis in accordance with such criteria. In addition, a covered entity may not use, disclose or request an entire medical record, unless the entire medical record is specifically justified as reasonably necessary to accomplish the purpose of the use, disclosure or request.

De-identified information

The privacy rule offers two methods through which a covered entity may de-identify protected health information. Once information is de-identified, it is no longer subject to the requirements of the rule. First, a covered entity may determine that individually identifiable health information is de-identified for purposes of the rule if (a) a qualified expert as described in the rule (b) determines that the risk of re-identification of the data, alone or in combination with other data, is very small and (c) documents the methods or results. Second, data is presumptively de-identified if the list of identifiers set forth in the rule are removed and the covered entity does not have actual knowledge that the information could be used, alone or in combination, with other data to identify an individual. The final rule also permits covered entities to develop codes for re-identification of de-identified data, provided that such codes are not related to or derived from information about the individual or otherwise capable of being translated so as to identify an individual patient and is not used or disclosed by the covered entity for any other purpose.

Research

Use and Disclosure of Personally Identifiable Information for Research Purposes

The privacy rule permits use or disclosure of health information for research purposes either with valid, written authorization, or with the approval of a properly constituted Institutional Review Board ("IRB"), or privacy board.

Authorization to Use Information in Research. The authorization may be combined with certain required notices and consents. Also, to be effective, an authorization must include specific descriptions of the information to be used or disclosed, the person or entity to whom disclosure may be made, and the purpose of the use or disclosure. In addition, it must include an expiration date, an explanation of how it may be revoked, and (if applicable) disclosure that the provider will receive remuneration from a third party for granting access to the information.

When information is created for "research that includes treatment," the authorization must also:

- describe the extent to which the health information will be used or disclosed for treatment, payment, or administrative purposes;

- explain which health information will be used or disclosed for hospital directories, public health purposes, and the like; and
- refer, if applicable, to the provider's Consent for Treatment and Notice of Privacy Policies.

Waiver of the Authorization Requirements. Under the final rule, covered entities are required to obtain documentation from researchers on the uses of protected health information in the research. An IRB or privacy board may alter or waive the authorization requirements under certain conditions. First, the IRB must be established and operate according to the Common Rule, and a privacy board must have similar composition and review procedures as described in the rule. Second, the board must document that it has determined each of the following:

1. the proposed use or disclosure presents no more than minimal risk to the individuals;
2. waiver of the authorization requirement will not adversely affect the privacy rights and welfare of the individuals;
3. the proposed research could not practicably be conducted without the waiver;
4. the research could not practicably be conducted without access to and use of the health information;
5. the privacy risks to the individuals are reasonable in relation to the anticipated benefits (if any) to them and the importance of the knowledge reasonably expected from the research;
6. an adequate plan exists to protect personal identifiers from improper use and disclosure;
7. an adequate plan exists to destroy such identifiers at the earliest opportunity consistent with conduct of the research (unless retention is justified by public health considerations or required by law); and
8. there are "adequate written assurances" that personally identifiable health information will not be reused or disclosed to a third party except as required by law, or for other research as permitted by the regulation.

In addition, documentation of a waiver must: identify the IRB or privacy board that approved the waiver; affirm that the IRB or privacy board made all of the determinations enumerated above; describe the information to which access has been approved; state whether the waiver was approved through normal or expedited review procedures; and be dated and signed by the Chair of the IRB or privacy board (or designee).

Notably, both the Privacy regulation and the Common Rule use the "impracticability" standard for waiver or alteration. It means more than merely inconvenient; rather, it requires a showing that the research, as a practical matter, could not be conducted without the waiver.

Access Without Authorization or Waiver

De-Identification. To avoid the need for authorization or waiver, information may be "de-identified," according to the criteria set forth in the above section on de-identification.

Reviews Preparatory to Research. Access to health information is permissible without authorization and without IRB or privacy board waiver if a researcher represents to the provider that: (1) access is sought solely to review the health information in order to prepare a research protocol or for similar purposes "preparatory to research"; (2) the information is necessary for research purposes; and (3) no protected health information will be removed

from the facility. The apparent purpose of this provision is to assist investigators in locating providers with patients who are likely to meet the eligibility criteria for a particular protocol.

Access to Decedents' Information. Access to health information of decedents is permitted for research purposes if a researcher represents to the provider that the information is sought solely for research related to the decedents' condition and is necessary for that research; and the researcher documents that the individuals whose records are sought are deceased.

Marketing

Under the final rule, health plans, health care clearinghouses and health care providers are prohibited from using or disclosing protected health information for marketing without specific patient authorization. The regulation, in effect, establishes two separate categories of marketing communications and rules governing the form of patient authorization required for each type. In addition, the regulation distinguishes "marketing" communications from the care management and benefits coordination activities that a health plan or health care provider may engage in the course of providing treatment or coordinating health benefits coverage and payment for an individual. The regulation also creates new rules for fundraising activities by certain not-for-profit entities. This advisory will briefly summarize each of these new regimes in turn.

Marketing by Covered Entities

The regulation accommodates the fact that health plans and providers also may engage in marketing activities and that their patient lists may sometimes be an acceptable source of contacts.[4] For communications by health plans and providers directly to patients, the regulation identifies very precise content and format requirements that must be met by any such communication, including a specific requirement that the covered entity provide an "opt-out" from all further marketing communications from the covered entity. Provided that the covered entity complies with these detailed new rules, these marketing communications by a covered entity may be encompassed by the consent or authority that the covered entity has for performing "health care operations."

Generally, a covered entity may not use or disclose protected health information for marketing without a valid authorization. Authorization is not required when communication to an individual occurs face-to-face with an individual, concerns products or services of nominal value, or concerns health-related products and services of the covered entity or a third party. However, these exceptions apply only when the communication

1. identifies the covered entity as the party making the communication;
2. prominently states whether the covered entity is receiving direct or indirect compensated for making the communication; and
3. describes how the individual may opt out of receiving future such communications (unless the communication is included in a broadly disseminated document such as a newsletter or pamphlet).

4. Important exceptions: If a covered entity has agreed to a more restrictive use of a patient's information (45 C.F.R. 164.522(a)), or has agreed to a confidential communication restriction (45 C.F.R. 164.522(b)), the regulation would not override the agreement to permit the covered entity to use the patient's contact information for marketing. (45 C.F.R. 164.502(h); 164.506(e).

These regulations do not authorize the covered entity to furnish its patient list to a third party for its marketing purposes.[5] Depending on the facts of the specific situation, any marketing communication by a covered entity that does not meet these narrow requirements would be a use or disclosure of protected health information in violation of the regulation, and would subject the covered entity to the civil and criminal penalties of the statute.

In addition, if a covered entity proposes to use patient information to selectively target its communication to individuals based on their health status or condition, the following requirements also must be met:

1. The covered entity must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and
2. The communication must explain why the individual has been targeted and how the product or service relates to the health of the individual; and
3. The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications are not sent such communications.

As noted above, any marketing communication by a covered entity that did not include this information, would be an impermissible use or disclosure of the patient information.

Care Management and Benefits Coordination

Under the regulation, the consent that the patient signs at the doctor's office or hospital covers "treatment" and "payment," which are defined to include various activities that providers and health plans perform in trying to ensure that patients receive medically appropriate care and that the care that is delivered is covered under the particular health benefits plan in which the patient is enrolled. Sometimes, the communications necessary to accomplish this may resemble "marketing" in that they concern specific products or the services of specific providers that are being recommended to the individual. Subject to the provisio discussed below, the regulation acknowledges this fact by excluding from the definition of "marketing" the following types of communications:

1. A communication made by a covered entity for the purpose of describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or
2. Communications tailored to the circumstances of a particular individual and that are made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual; or
3. Communications made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

---

5. A covered entity may contract with a "business associate" to prepare its marketing communications, but business associates must be prohibited from using or disclosing the information for any purpose not specifically authorized by the covered entity and permitted by the regulations, and are subject to other safeguards such as a requirement that health information be returned to the covered entity at the conclusion of the business associate's assigned tasks.

A communication of any of these three types is not marketing only if (1) the communication is made orally, or (2) the communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.

Under the regulation, a communication that does not meet these narrow criteria to be considered part of the arrangements for treatment and benefits administration, is "marketing" and, if the communication is made by a covered entity, it must comply with the regulation's requirements regarding content and form (discussed above), and must provide for an opt-out of future marketing communications. And if the communication is made by a third party, the patient's specific authorization must have been obtained in advance for use of the protected health information in making the communication.

Marketing by Third Parties

The regulation 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 the product or service."[6] Any disclosure of patient information, including a list or roster of a provider's patients, to a third party for marketing is explicitly prohibited by the rule without the specific authorization of each patient. The authorization form must specify the purpose of the disclosure, the information to be disclosed and the third party recipients. The availability of treatment and payment cannot be conditioned on signing of such an authorization; and the authorization cannot be in the same form in which the patient provides consent for information to be used in providing treatment. The authorization must have an expiration date, and be revocable by the patient at any time. The covered entity must keep a list of all of the third parties to which the patient's information has been disclosed under such an authorization, and the patient has the right to obtain a list of all of those disclosures.

Fundraising

The regulation acknowledges the fact that some covered entities are not-for-profit entities that must engage in fundraising in order to support their basic activities. Patients and former patients often are receptive and respond generously to fundraising requests. The regulation does not treat these activities as "marketing," but as a special, very limited use of certain information permitted under separate, specific rules governing the "health care operations" of the not-for-profit entity.[7] To be permissible as "fundraising" the communication must meet all of the following criteria:

1. The covered entity (its business associate) or an institutionally related foundation must make the communication;
2. Only demographic information relating to an individual, and dates of service (not information about health or health care) may be used or disclosed for fundraising;
3. The information may be used to raise funds only for the benefit of the covered entity that has authority to use the information for treatment, payment, and health care operations with respect to the individual;
4. Any fundraising materials sent to the individual must include a description of how the individual may opt out of receiving any further fundraising communications; and

6. 45 C.F.R. 164.501.
7. 45 C.F.R. 164.514(f).

5. The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

As noted above, any use or disclosure of patient demographic information for fundraising activities that does not comply with these requirements would be a prohibited use or disclosure of protected health information under the regulation. If the covered entity did not obtain the specific authorization of the patient for such non-conforming fundraising activities, the use or disclosure of the information in the fundraising activity would be subject to civil and/or criminal sanctions under HIPAA.

Patient rights

In addition to requiring that patients be given accurate and binding advance notice of the uses that each covered entity will make of their medical information, the final rule establishes certain rights for individuals who are the subject of protected health information, and standards and procedures for the exercise of those rights. These rights include the right to obtain access to protected health information about themselves, the right to request amendment or correction of protected health information, the right to request confidential communications, and the right to an accounting of disclosures. Individuals would also be able to request that a covered entity restrict their protected health information from further use or disclosure for treatment, payment or health care operations.

Pre-emption

The final rule creates a federal floor of privacy protection, but would not supercede laws that provide greater protection for the confidentiality of health information.

Transition provisions

The final rule also includes provisions that apply to the use or disclosure of protected information by covered entities pursuant to a consent or authorization that is obtained from an individual before the compliance date of the rule, and that does not comply with the rule's consent/authorization requirements. Generally, a covered entity may rely on such consents or authorizations with respect to protected health information that it creates or receives before the compliance date, provided that it does not make any use or disclosure that is expressly excluded from the consent or authorization and complies with all limitations included in the consent or authorization.

Effective dates

For purposes of the civil and criminal penalties imposed under Title XI of the Social Security Act, covered entities would need to be in compliance with the standards promulgated in the final rule by two years after the effective date of April 14, 2001. After that date, providers may continue to rely on prior written authorizations for the use or disclosure of personally identifiable information (even if the authorizations do not comply with all the requirements of the Privacy regulation) so long as the use or disclosure does not exceed the express purpose(s), or violate any explicit limitations, of the prior authorization. Small health plans will have an extra year to come into compliance.

Penalties for violations

Knowing violations of the regulations are subject to civil monetary penalties of up to $100 for each violation, capped at $25,000 for all violations of the same provision in a calendar year.[8] Violators also may be subject to criminal prosecution resulting in fines of up to $50,000, imprisonment for up to one year, or both. If the offense is committed under false pretenses, the violator may be fined up to $100,000, imprisoned for up to five years, or both. Finally, if the offense is committed with "intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm," the violator may be fined up to $250,000, imprisoned for up to ten years, or both.[9]

Conclusion

Hogan & Hartson attorneys with considerable experience advising clients with respect to HIPAA issues can offer many pragmatic tools and services necessary to assist in compliance with these new and complex rules.

This focus on medical privacy regulations was compiled from a series of advisories that were prepared by Hogan & Hartson attorneys regarding the HIPAA privacy regulations. It is for information purposes only and is not intended as a basis for decisions in specific cases. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship.

Donna Boswell and Marcy Wilder are partners in the firm's Health Group. Partner Barbara Mishkin and associates Nalini Anand, Bart Barefoot, Melissa Bianchi, Tracy-Elizabeth Clay, and Melissa Levine also contributed to the writing of this piece.

For more information, please contact the following Hogan & Hartson attorneys:

Donna Boswell *Washington, DC*
202/637-5814
daboswell@hhlaw.com

Marcy Wilder *Washington, DC*
202/637-5729
mwilder@hhlaw.com

8. 42 U.S.C. §1320d-5.
9. Id. § 1320d-6.