Davis Wright Tremaine LLP

A HOLIDAY GIFT FROM HEALTH & HUMAN SERVICES: FINAL HIPAA PRIVACY REGULATIONS CONTAIN SIGNIFICANT CHANGES

A Holiday Gift from Health & Human Services: Final HIPAA Privacy Regulations Contain Significant Changes

In a closely watched development, the Department of Health and Human Services ("DHHS") issued final privacy regulations for electronic health information on Wednesday, December 20, 2000. More than 100 pages in length and accompanied by more than 1400 pages in commentary, the regulations impose a massive and complex burden on providers, health plans and clearinghouses, as well as their business associates.

The regulations were issued pursuant to requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). DHHS had published a proposed privacy rule in November 1999 and in response received more than 50,000 comments. Based on those comments, DHHS made significant changes to the proposed privacy rule. The final regulations will go into effect in February, 2003, although small health plans will have an additional year to comply.

HIGHLIGHTS OF THE FINAL REGULATIONS

- The most significant change is that the regulations now extend to all individually identifiable health information in the hands of covered entities, regardless of whether the information is or has been in electronic form. This includes purely paper records and oral communications. In contrast, the proposed rule only covered information that had at some point existed in electronic form. The difficulty of tracking electronic and non-electronic information had convinced many observers that the distinction made in the proposed rule was unworkable, but there are concerns that HIPAA may not authorize this expansion of the regulations' coverage.

- Business partner agreements (now called business associate contracts) need no longer give patients direct rights over health care information in the hands of a covered entity's business associate. In addition, the final regulations also withdrew from the proposed rule a hotly debated requirement that business associate contracts declare patients to be "third-party beneficiaries" of the contract.

- The final regulations clarify that covered entities are not required to actively monitor business associates for compliance with their contracts, although they must take action if they know of practices that violate the agreement. The regulations also clarify that physicians on hospital medical staffs are not, by virtue of their staff membership, business associates of the hospital.

- The final regulations introduce the concept of an "organized health care arrangement," which is a clinically integrated setting in which patients receive care from more providers than one, or an organized system of health care, or a combination of group health plans or group health plans and insurers. Participants in an organized health care arrangement are permitted to use and disclose information for the health care operations of the arrangement,

just as they are for their own health care operations. Participation in an organized health care arrangement does not, in and of itself, make the participants business associates of one another.

- Subject to limited exceptions, providers and other covered entities will need to obtain a patient's "consent" to the entity's disclosure of the patient's health information for treatment, payment and the entity's own operations. This is a significant shift from the proposed rule, which would have permitted such use of information without the patient's authorization.

- Providers will be pleased to know that the regulations permit them to use limited patient information, without patient authorization, in connection with their fundraising activities, including fundraising by related foundations.

- The final regulations retain the "minimum necessary" standard first set forth in the proposed rule, under which a disclosure of protected health information, even where authorized by the regulations, must be limited to the "minimum necessary" to accomplish the purpose for which it is made. However, under the final regulations, this determination does not have to be made when responding to a request from another covered entity. Instead, the final rule states that a covered entity requesting protected health information from other covered entities must limit its request to what is reasonably necessary to accomplish the purpose for which the request is made.

- The final regulations include new requirements relating to disclosures of protected health information by group health plans. "Group health plans" include insured and self-insured plans sponsored by employers, and other employee welfare benefit plans subject to ERISA (however, self-administered plans having fewer than 50 participants are not covered). In order for a group health plan to share protected health information with a plan sponsor—typically, the employer—there must be specific restrictions on the sponsor's use and disclosure of the information. For example, the sponsor must restrict access to protected health information to employees who perform health plan administrative functions on behalf of the sponsor.

- The final regulations continue the special requirements for use of protected health information for research purposes, requiring approval by an Institutional Review Board or a privacy board. However, the requirements in the final regulations are more comprehensive and restrictive than in the proposed rule.

- Enforcement of the privacy regulations has been delegated to the DHHS Office of Civil Rights. The regulations do not provide for a private right of action that would permit patients to sue for violations, but there are both civil and criminal penalties for violation, including a fine of up to $250,000 and imprisonment for up to 10 years for knowingly disclosing or obtaining protected health information if done for commercial or personal gain or for malicious harm.

SUMMARY OF PRIVACY FEATURES

Covered Entities

Like the proposed rule, the final regulation applies to health plans and health care clearinghouses, and to health care providers that electronically transmit health information in connection with standard transactions (such as a claim for payment).

- "Health plan" generally includes any individual or group plan, private or governmental, that provides or pays for medical care. Employee health benefit plans are excluded if they are self-administered and have fewer than 50 participants. Government-funded programs are excluded if their principal purpose is something other than providing or paying for health care, or if their principal activity is the direct provision of health care or the making of grants to fund health care.

- "Health care clearinghouse" is a public or private entity that processes health information received from another entity from non-standard into standard format, or vice versa. The regulations distinguish between a clearinghouse dealing with information in its own right (in which case it is bound by all the requirements of the regulations), and in its capacity as a business associate of another covered entity (in which case some of the requirements do not apply, but it is bound by its business associate contract with the covered entity). For example, the patient rights provisions would be enforced through the business associate contract, not directly.

- "Health care provider" is any person or organization who furnishes, bills or is paid for health care in the normal course of business. However, health care providers are covered by the rules only if they transmit electronic health information in connection with a standard transaction.

An entity that fits more than one definition must comply with the rules as they affect each of its functions, and may use or disclose information only as appropriate to the function for which the use or disclosure is made.

Covered Health Information

The regulation protects individually identifiable health information transmitted or maintained in any form or medium ("protected health information" or "PHI"). This excludes only education records and student medical records. Individually identifiable health information is health information (including demographic information) that identifies or can be used to identify the individual. "Health information" is broadly defined to include any information, oral or recorded, relating to the health of an individual, the health care provided to an individual, or payment for health care provided to an individual.

The regulations do not apply to health information that has been "de-identified" by removing, coding, encrypting, or otherwise eliminating or concealing all individually identifiable information. De-identified information may be used or disclosed freely so long as no means of

re-identification is disclosed. Information is presumed to be de-identified if all the following are removed: names, geographic designations smaller than a State, dates, telephone, fax and other identifying numbers, addresses, URLs and IP addresses, biometric identifiers, identifiable photographs, and other unique identifiers. If all of these identifiers are not removed, information can still be treated as de-identified if a qualified statistician determines that the risk of re-identification is very small.

Use and Disclosure

The general rule is that patient health information may not be used or disclosed unless the disclosure is either authorized by the patient (or someone able to act on the patient's behalf) or is specifically required or permitted under the HIPAA regulations. This approach is similar to that used in many State statutory schemes. However, because HIPAA preempts contrary State laws, the privacy regulations will provide a generally uniform minimum level of confidentiality protection for health information (more stringent State laws are permitted).

The final regulation permits limited use and disclosure of protected health information without consent or authorization in a variety of circumstances where there is an overriding public interest. These include disclosure for public health activities and other governmental functions, for medical research, to report abuse or neglect, for judicial and law enforcement purposes, and the like. Each ground for disclosure is subject to specific limitations on the type of health information that can be released, the purpose for which it may be released, and the persons to whom it may be released. The regulations also include special, more restrictive rules for the disclosure of psychotherapy notes and research information unrelated to treatment.

Except where the HIPAA regulation requires or permits release of patient information (e.g., reports of child abuse or infectious diseases), covered entities must obtain written permission from patients for use or disclosure of their information. A general "consent" is required for use or disclosure of information for treatment, payment and the covered entity's own health care operations. This consent can be written in general terms and refer to the entity's own privacy practices. Where a patient's health information is to be used or disclosed for specific purposes other than treatment, payment or health care operations, a more specific written permission – an "authorization" – is required. Covered entities may refuse to treat or cover individuals who refuse to give a general consent to the use of their information for treatment, payment and health care operations purposes, but in most cases they may not refuse treatment or coverage when the patient refuses to authorize other uses or disclosures.

The regulations include detailed requirements for the content of forms authorizing the release of protected health information. For example, all "authorization" forms must contain certain core elements, whether the request for disclosure is made by an individual or a covered entity. Additional requirements apply to forms used when a covered entity seeks authorization for its own uses or for disclosure to another covered entity. This differs from the approach taken in the proposed rule. Unlike the proposed rule, the final regulations do not include a model authorization form. The commentary to the final regulations clarifies that an authorization form may be signed with an electronic signature when DHHS adopts electronic signature standards.

Patient Rights

Right to adequate notice of privacy practices

Patients have a right to receive a notice describing the covered entity's privacy practices. The notice must also inform patients how to file complaints, either with the covered entity or DHHS, and identify a contact person who can provide additional information. The notice should describe how the covered entity will provide patients with a revised notice if the notice is changed. Rather than require health plans to issue their notices to enrollees every three years, the final regulations require plans to inform enrollees every three years about the availability of the notice and how to obtain a copy.

Right to access health information

Patients have a right to access, inspect, and copy protected health information that is used, in whole or in part, to make decisions about them. Access is available for as long as the health information is maintained by the covered entity in a designated record set. Patients do not, however, have an automatic right of access to psychotherapy notes; information compiled for use in a civil, criminal, or administrative action or proceeding; and certain health information maintained by a covered entity that is subject to or exempted from the Clinical Laboratory Improvements Amendments ("CLIA") of 1988.

The regulations include limited grounds for denial of patient access to their own health information. Any denial of access must be accompanied by information on how to have the denial reviewed or on how to make a complaint either to the covered entity or DHHS. Covered entities must act on a request for access within 30 days of receiving the request if the information is maintained or accessible on-site (otherwise within 60 days). Fees may be charged, but only for copying and mailing costs.

Right to request amendment of health information

A patient has the right to request amendment of protected health information. A covered entity may deny this request if the information is accurate and complete or was not created by the covered entity. If the amendment is denied, the covered entity must inform patients of their options with respect to future disclosures of the disputed information.

Right to an accounting of disclosures

Patients have a right to receive an accounting of disclosures made by a covered entity for purposes other than treatment, payment, and health care operations made within six years prior to the request. Covered entities are not required to include in the accounting certain disclosures, such as disclosures for national security or intelligence purposes, disclosures to law enforcement officials; or disclosures made prior to the compliance date for the final regulation. The accounting must include a brief statement of the purpose of the disclosure and the address of the recipient of the disclosed information. The accounting must be provided within 60 days after

receipt of the request. Patients have the right to receive one free accounting every twelve months. Covered entities may charge a reasonable, cost-based fee for additional accountings.

Right to request restriction of uses and disclosures

Patients have the right to request restrictions on the use and disclosure of their protected health information. Covered entities are not required to agree to these requests, but if they do, they must abide by them, except in emergencies. A covered entity must document any restriction to which it agrees and maintain the documentation for at lease six years.

Right to request restrictions communicating health information

Patients may ask health care providers and plans to communicate health information to them by "alternative means" or at "alternative locations." Providers must accommodate these requests if they are reasonable. Health plans need not accommodate them unless the individual clearly states that disclosure of the information could endanger the individual.

Business Associates

A covered entity may disclose protected health information to its business associates without further authorization if it obtains satisfactory assurances, through a written contract, that the business associate will appropriately safeguard the information. A business associate is someone who performs or assists the covered entity to perform a function of the covered entity, or who provides services to the covered entity. A covered entity does not need a business associate contract with members of its own workforce. The business associate contract must contain specified provisions addressing the restrictions on the business associate's use and disclosure of the health information transferred to it.

A business associate may use protected health information for its own management and administration, and may disclose it to others if it obtains assurances that the information will be held in confidence and that the recipient will notify the business associate of breaches of confidentiality.

A covered entity is responsible for violations by its business associate if it knew of a pattern of activity or practice that constituted a material breach of the contract, and failed to take reasonable steps to end the violation (e.g., contract termination or notification to DHHS of the problem).

Administrative Procedures

Covered entities must have policies, procedures and systems in place to protect health information and individual rights. Requirements include: designation of a privacy officer; privacy training for employees; safeguards to prevent intentional or accidental misuse of protected health information; and sanctions for employee violations of those requirements.

The final regulations are less prescriptive than the proposed rule with respect to employee training requirements. Covered entities are now required to document that training requirements have been satisfied, rather than having their employees sign a certification form upon completion of training and once every three years thereafter.

Preemption of State Law

The federal regulations preempt all "contrary" state laws unless a state law is more stringent. A state law is contrary to the federal standard when an entity would find it impossible to comply with both the state and federal requirements or when the state law is an obstacle to the accomplishment of the purposes and objectives of HIPAA.

A state law is more stringent than the federal standard if the state law: further limits the use or disclosure of protected health information (although a state may not place further limits on the rights of individuals to their health information); provides individuals with greater rights of access to their health information (with exceptions for minors), or more information about their rights; enhances the protection afforded by an authorization for use or disclosure of health information; imposes greater record-keeping requirements; or otherwise enhances privacy protection.

In addition, a state law is not preempted if DHHS determines that it is necessary for the administration of health care, to serve a compelling need related to public health, safety or welfare, or to regulate controlled substances; or if the law relates to certain state reporting requirements. States can apply to DHHS for a determination whether a state law meets the requirements of these exceptions.

FOR MORE INFORMATION ON HIPAA

- Check the Davis Wright Tremaine website:

  http://www.dwt.com/practc/hc_ecom/hc_ecom.htm

- Send us an email at: HIPAA@dwt.com