

HEALTH PRIVACY REGULATIONS WILL AFFECT HEALTH PLANS

D. Robert Enten, Esq.
Christine Williams, Esq.
(410) 576-4000

On April 12, 2001, the Secretary of the U.S. Department of Health & Human Services (“HHS”) announced that health privacy regulations issued by the Clinton administration in December 2000¹ would go into effect as scheduled on April 14, 2001. The regulations require “covered entities” to comply with new privacy standards that were issued as part of the “administrative simplification” provisions of the Health Insurance Portability and Accountability Act (“HIPAA”).²

“Covered entities” include health plans that are sponsored by employers and health care providers that choose to transmit protected health information by electronic means.³ Most covered entities will be required to comply with the new standards by April 14, 2003.⁴

The HHS announcement noted that there would be clarifying guidelines, or recommended modifications, in three specific areas: sharing information among the doctors and hospitals treating a patient, efficient delivery of patient care unhampered by the requirements surrounding consent forms, and parent access to health information relating to their children. The first such guidance was issued on July 6, 2001.⁵ However, regardless of the clarifications and modifications, the privacy standards will require major changes in the policies and operations of covered entities, and will give significant new rights to patients and plan participants.

Protected Health Information

The regulations cover “protected health information” (“PHI”) held by covered entities. PHI is information that is individually -identifiable and that relates to a medical condition, treatment, or payment for health care.⁶ The regulations cover all PHI, regardless of whether it is oral, on paper, or in electronic form.⁷

Consents and Authorizations

Covered entities may not use PHI internally, or disclose PHI to others, unless permitted to do so by the regulations⁸ or by the patient or enrollee.⁹ In general, PHI may be used or disclosed by a provider for treatment, payment, or health care operations¹⁰ only if the patient or enrollee signs a “consent.”¹¹ Other covered entities may use and disclose PHI for treatment, payment, or health care operations without a consent.¹² Use or disclosure of PHI by any covered entity for purposes other than treatment, payment, or health care operations is permitted only if the patient or enrollee signs an “authorization.”¹³ Under the new regulations, a “consent” and an “authorization” have different requirements and functions.

A “consent” is a short, general form that allows use and disclosure of PHI for treatment, payment, and health care operations. It must be written in plain language and must include the following:

1. A reference to the covered entity’s notice of privacy policies and procedures and a statement that the patient or enrollee has the right to review the notice before signing the consent;
2. If the covered entity has retained the right to change its privacy policies and procedures, a statement to that effect and a description of how the patient or enrollee may obtain a revised notice;
3. A statement that PHI may be used and disclosed for treatment, payment, or health care operations and that the patient or enrollee has the right to request restrictions on use and disclosure for such purposes, but that the covered entity is not required to agree to such a request;
4. A statement that the patient or enrollee has the right to revoke the consent, if done so in writing.¹⁴

A consent must be signed by the patient or enrollee, and must be dated.¹⁵ In general, a health care provider may refuse to treat a patient if the patient refuses to sign a consent, and a health plan may refuse to enroll a person who refuses to sign a consent.¹⁶

An “authorization” is a longer, more detailed form that allows use and disclosure of PHI for purposes other than treatment, payment, and health care operations. All authorizations must be written in plain language and must include the following:

1. A specific description of the information to be used or disclosed;
2. Name or other specific identification of the persons authorized to use or disclose the PHI;
3. Name or other specific identification of the persons to whom the covered entity is authorized to make the disclosure;
4. An expiration date or event;
5. A statement that the patient or enrollee has the right to revoke the authorization, if done so in writing;
6. A statement that when the PHI is used or disclosed under the authorization, it may no longer be protected by the regulations.¹⁷

An authorization must be signed by the patient or enrollee, and must be dated.¹⁸ If it is signed by a representative of the patient or enrollee, there must be an indication of the representative’s authority to act for the patient or enrollee.¹⁹

If the authorization is requested by the patient or enrollee, there are no other requirements. However, if the authorization is requested by the covered entity for its own uses and disclosures, or for uses and disclosures by others, there are additional requirements and additional information that must be included in the authorization.²⁰ In general, a health care provider may not refuse to treat a patient if the patient refuses to sign an authorization, and a health plan may not refuse to enroll a person who refuses to sign an authorization.²¹

Both consents and authorizations must be retained by the covered entity for at least six years from the later of the date of creation or the date they were last in effect.²²

Other Compliance Obligations

In addition to limiting uses and disclosures of PHI to what is permitted by the regulations and consents and authorizations signed by patients or enrollees, covered entities are required to:

1. Adopt and implement written privacy policies and procedures;²³
2. Enter into contracts with business associates that receive PHI from the covered entities requiring the business associates to comply with the same standards as the covered entities;²⁴
3. Provide a notice of privacy policies and procedures to patients or enrollees;²⁵
4. Train employees in the privacy policies and procedures;²⁶
5. Appoint a privacy officer;²⁷ and
6. Disclose only the “minimum necessary” PHI for the particular purpose.²⁸

The definition of “business associates” is broad, and includes any person to whom PHI is disclosed if that person performs or assists in the performance of functions such as claims processing, billing, benefit or practice management, and quality assurance, or provides legal, actuarial, accounting, consulting, management, administrative, accreditation, or financial services.²⁹ The breadth of the definition is of particular importance to attorneys who represent covered entities, as they will often fall within the definition of “business associates” and will be required to sign agreements by which they agree to abide by the same privacy standards that apply to their clients.

An employer-sponsored health plan may not disclose PHI to the employer unless specified amendments to the plan documents are adopted, limiting the employer's use and disclosure of the PHI.³⁰

Patient and Enrollee Rights

Patients and enrollees have a right to receive a copy of the covered entity's notice of privacy policies and procedures, and patients and enrollees have the right to:

1. Inspect and obtain a copy of their PHI;³¹
2. Request amendment of their PHI;³²
3. Receive an accounting of disclosures of PHI other than those for treatment, payment, and health care operations;³³ and
4. Request that uses and disclosures of PHI be restricted.³⁴

Penalties

Criminal penalties for non-compliance include fines of up to \$250,000 and up to 10 years in prison for violations that are knowing and intended for commercial advantage or malicious harm.³⁵ Civil penalties of up to \$100 per violation may be imposed, up to a maximum of \$25,000 per year for violations of the same requirement or prohibition.³⁶ There are more than 50 separate requirements and prohibitions in the regulations, so civil penalties could approach \$1.5 million in one year for a single covered entity.

The regulations do not provide for suits by patients or enrollees against covered entities. However, the new standards may become the measuring rod for what is "reasonable care" in handling health information,³⁷ and state courts may use the standards to gauge whether health care providers and health plans have acted reasonably in dealing with health information. This could open covered entities to suits in state court under state law.³⁸

Relationship to State Laws

The HIPAA privacy standards establish a floor, rather than a ceiling. If the federal standards are more stringent than state law, the federal standards apply. However, if the covered entity is subject to state law and the state law gives patients or enrollees greater protection, the state law applies.³⁹ For example, a self-funded health plan is not subject to state law and will only be covered by the federal standards. On the other hand, an insured health plan may be subject to state law and must comply with the federal standards as well – if the state law gives participants more protection than the federal standards, the state law will apply; if the federal standards give participants more protection, the federal standards will apply. This means that covered entities that are subject to state law will have to comply with a patchwork of state and federal law.

Preparing for Compliance

Compliance with the new standards will require more than paperwork. Most covered entities will have to redesign at least some aspects of their operations, and some covered entities will have to make major changes. The first steps on the road to compliance include:

1. A thorough inventory of the covered entity's records to determine what PHI it holds, who has access to it, who it is disclosed to, and what it is used for;
2. A review of the inventory to determine to what extent the covered entity is not in compliance with the new standards; and
3. An examination of the areas of non-compliance to determine how procedures and operations may best be changed to achieve compliance, while still meeting the covered entity's operational needs.

Although the compliance deadline of April 2003 seems a long way off, the new standards are complex, and a redesign of operations and procedures takes thoughtful preparation. As the July guidance from HHS put it,

“Covered entities can and should begin the process of implementing the privacy standards in order to meet their compliance dates.”⁴⁰

Endnotes

1. 65 Fed. Reg. 82462 (12/28/00).
2. 42 U.S.C. § 1320d et seq.
3. 45 C.F.R. § 160.103, 65 Fed. Reg. 82799. Also included are health care clearinghouses, which are entities that translate health care transaction data from nonstandard to standard format, or vice versa. 45 C.F.R. § 160.103, 65 Fed. Reg. 82799.
4. Small health plans, defined as those with \$5 million or less in annual receipts, 45 C.F.R. § 160.103, 65 Fed. Reg. 82800, have until April 14, 2004. Among health plans, only those that (1) have fewer than 50 participants, and (2) are administered by the plan sponsor, are excepted from the regulations. 45 C.F.R. § 160.103, 65 Fed. Reg. 82799.
5. <http://www.hhs.gov/ocr/hipaa/finalmaster.html>. The guidance states that changes to the regulations will be proposed to permit pharmacists to fill prescriptions phoned in by a physician before the pharmacist obtains the patient’s written consent and to permit a friend or relative of the patient to pick up the prescription; to permit a provider to schedule an appointment before obtaining the patient’s written consent; to permit “whatever communications are required for quick, effective, high quality health care;” and to assure covered entities that common practices such as the use of sign-up sheets, x-ray lightboards, and maintenance of patient charts at bedside are not prohibited.
6. 45 C.F.R. § 164.501, 65 Fed. Reg. 82804 and 82805 (“individually identifiable health information” and “protected health information”).
7. 45 C.F.R. § 160.103, 65 Fed. Reg. 82799.
8. 45 C.F.R. § 164.512, 65 Fed. Reg. 82813 (e.g., for public health activities, judicial and administrative proceedings, law enforcement purposes, etc.).
9. 45 C.F.R. § 164.502(a), 65 Fed. Reg. 82805.
10. “Health care operations” is a defined term, and is limited to quality assessment and improvement activities; training and evaluation, including accreditation and similar activities; underwriting and premium rating relating to insurance and reinsurance; conducting or arranging for medical review, legal services, and auditing, including fraud and abuse detection; and business planning and management. 45 C.F.R. § 164.501, 65 Fed. Reg. 82803-804.
11. 45 C.F.R. § 164.506(a), 65 Fed. Reg. 82810.
12. *Id.*
13. 45 C.F.R. § 164.508(a), 65 Fed. Reg. 82811.
14. 45 C.F.R. § 164.506(c), 65 Fed. Reg. 82810.
15. *Id.*
16. 45 C.F.R. § 164.506(b), 65 Fed. Reg. 82810.
17. 45 C.F.R. § 164.508(c), 65 Fed. Reg. 82811-12.

18. *Id.*
19. *Id.*
20. 45 C.F.R. § 164.508(d) and (e), 65 Fed. Reg. 82812.
21. 45 C.F.R. § 164.508(b), 65 Fed. Reg. 82811.
22. 45 C.F.R. §§ 164.506(b), 164.508(b), 164.530(j), 65 Fed. Reg. 82810, 82811, 82828.
23. 45 C.F.R. § 164.503(i), 65 Fed. Reg. 82827.
24. 45 C.F.R. § 164.502(e), 65 Fed. Reg. 82806.
25. 45 C.F.R. § 164.520, 65 Fed. Reg. 82820.
26. 45 C.F.R. § 164.530(b), 65 Fed. Reg. 82826.
27. 45 C.F.R. § 164.530(a), 65 Fed. Reg. 82826.
28. 45 C.F.R. § 164.502(b), 65 Fed. Reg. 82805.
29. 45 C.F.R. § 160.103, 65 Fed. Reg. 82798-99.
30. 45 C.F.R. § 164.504(f), 65 Fed. Reg. 82809.
31. 45 C.F.R. § 164.524, 65 Fed. Reg. 82823.
32. 45 C.F.R. § 164.526, 65 Fed. Reg. 82824.
33. 45 C.F.R. § 164.528, 65 Fed. Reg. 82826.
34. 45 C.F.R. § 164.522(a), 65 Fed. Reg. 82822.
35. 42 U.S.C. § 1320d-6.
36. 42 U.S.C. § 1320d-5.
37. *E.g., U.S. v. Sutherland* (W.D. Va. 2001), <http://www.vawd.uscourts.gov/opinions/jones/sutherland1.pdf> (in criminal prosecution of doctor for unlawful distribution of controlled substances, court looked to HIPAA privacy regulations for guidance on appropriate privacy protection for patients' whose records had been subpoenaed).
38. *E.g., Dishman v. UNUM Life Ins. Co.*, 2001 U.S. App. LEXIS 8529 (9th Cir., 5/8/01) ([http://www.ca9.uscourts.gov/ca9/newopinions.nsf/2420941536B4FA2588256A46005D0DED/\\$file/9955963.pdf?openelement](http://www.ca9.uscourts.gov/ca9/newopinions.nsf/2420941536B4FA2588256A46005D0DED/$file/9955963.pdf?openelement)) (permitting a state law invasion of privacy claim against an ERISA disability plan to go forward, holding that the claim was not preempted by ERISA).
39. 45 C.F.R. § 160.203, 65 Fed. Reg. 82801.
40. <http://www.bhs.gov/ocr/hipaa/finalmaster.html> at p. 5.