Pain Physician, Volume 5, Number 4, pp 433-439
2002, American Society of Interventional Pain Physicians®
ISSN 1533-3159

Health Law Review

Keeping Pace with HIPAA's Changes: Straight Talk from the Trenches

Erin Brisbay McMahon, JD

Over the past several months, the Department of Health and Human Services (DHHS) has issued new final and proposed rules pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The privacy rule was finalized on August 14, 2002. Changes made to the original rule were in general beneficial to providers. Consent forms will no longer be required for treatment, although providers may choose to continue to use them. Physicians will still be required to use and disclose only the "minimum necessary" protected health information (PHI) to accomplish the purpose for which the information is being used or disclosed, but the new final rule excludes some situations in which the minimum necessary requirement will apply. A model business associates contract is provided in the final rule, making it easier for providers to comply with the rule's requirement that they have written business associate contracts with vendors who need access to the provider's PHI to perform tasks on behalf of providers. Researchers now only need to provide one form for consent and authorization, instead of two.

There are also proposed changes in the transaction rule. Certain data elements that were required by the final rule are now situational in the proposed rule. Unnecessary data elements have been removed. Certain items, like special program indicator codes, will now be able to be reported via external code sets rather than as data elements in a transaction. The proposed rule also adopts requests from the industry by adding data elements, codes, or loops to enable covered entities to perform certain business functions in the standardized transactions, such as cross-referencing two subscriber IDs (e.g., surviving spouse and dependents).

A final rule was published in May 2002 that created a standard employer identifier. The Employer Identifier Number (EIN) that is already in use by the IRS will be the standardized unique employer identifier number.

A proposed rule to cease using the National Drug Codes in transactions for nonretail pharmacy transactions was published in May 2002. DHHS developed the proposal in response to widespread industry concern over the tremendous cost of implementing the National Drug Codes (NDC). The NDC will either not be replaced at all, or will be replaced by the HCPCS.

This article is not, and should not be construed as, legal advice or an opinion on specific situations.

Keywords: HIPAA, privacy, transactions, code sets, NDC, employer identifier

Congress required the Department of Health and Human Services (HHS) to develop patient privacy protections as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In December 2000 the "final" privacy rule was published. In March 2002, HHS proposed specific changes to the privacy rule in response to comments from the health care industry and patient advocacy groups. The proposed changes were analyzed, and a new "final" rule was issued on August 14, 2002. The date that providers must be in compliance with the privacy rule did not change: it remains April 14, 2003.

The major changes between the old final rule and the new final rule affected the areas of consent and notice, patient rights and protections and assistance for providers.

CONSENT AND NOTICE

Consent forms to use and disclose protected health information (PHI) for treatment, payment, and health care operations are no longer required. The industry successfully argued that the consent requirements interfered with the delivery of health care. Specifically, pharmacists complained that the consent requirements interfered with filling prescriptions for patrons who did not have a consent on record, and providers complained

From the law firm of Wyatt, Tarant & Combs, LLP, Lexington, Kentucky. Ms. McMahon is an attorney at Wyatt, Tarant & Combs. Address correspondence: Erin Brisbay McMahon, Esq., 250W. Main St, Suite 1600, Lexington, KY 40502. E-mail: emcmahon@wyattfirm.com

that the requirement interfered with referrals and providing treatment over the telephone.

Under the new final rule, providers will have to ask patients to provide written acknowledgment that they received a Notice of Privacy Practices. Providers must use good faith efforts to obtain the written acknowledgement. If a patient refuses to sign or otherwise fails to provide an acknowledgement, then a provider must document its good faith efforts to obtain the acknowledgement and the reason the acknowledgement was not obtained. This requirement is waived only if the patient presents in an emergency treatment situation. Even then, the patient must be given a copy of the Notice of Privacy Practices as soon as is practicable after the emergency situation has passed (1).

A provider does not have to get its patients to sign the Notice of Privacy Practices (which typically average from 3-25 pages). The preamble to the final regulations states that providers may have patients sign a separate sheet or list, or initial a copy of the first page of the notice and return it to the provider. If a provider chooses to use consent forms, the acknowledgement of receipt of the Notice of Privacy Practices may be combined with the consent form (2).

Physicians should be aware that the Notice of Privacy Practices must be delivered to patients upon the first service delivery, even if the first service delivery is via telemedicine. The government expects that if the Notice of Privacy Practices is delivered electronically, the provider's computer system must be capable of capturing the individual's acknowledgement of receipt electronically. If a practice plans to deliver services electronically, it should print out any evidence of receipt and place it in the patient's chart.

PATIENT RIGHTS

Marketing

The definition of marketing in the December 2000 rule focused on the intent of the communication, i.e., was a purpose of the communication to encourage recipients to purchase or use a product or service? This subjective definition was deleted from the new final rule, which defines marketing as either:

(1) making a communication about a product or service that encourages recipients to purchase or use the product or service; or

(2) an arrangement between a covered entity (including a provider) and any other entity in which the covered entity discloses PHI to the other entity in exchange for remuneration so that the other entity or its affiliate can communicate about its own product or service in a way that encourages recipients to purchase or use the product or service (3).

Under the new rule, all marketing communications require a written authorization from the patient except for face-to-face communications between providers and patients or situations in which the communication involves a promotional gift of nominal value (4). What is nominal value? The high end of the range probably tops out at fifty dollars, but that is being quite generous. Note that blanket marketing authorizations are defective and can lead to penalties under HIPAA (5). The new rule eliminates the opportunity providers had under the old rule to avoid obtaining an authorization by, among other things, giving the patient the opportunity to opt out of future communications.

Exclusions from the Definition of Marketing

Under the new final rule, even if a communication is made about a product or service that encourages recipients to purchase or use the product or service, it is excluded from the definition of marketing if it is made by a provider for:

(1) treatment of a patient; or
(2) case management or care coordination for the patient, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the patient (3).

The old rule had similar exclusions, but the exclusions only applied if the communication was oral or, if in writing, the provider received no remuneration. These restrictions on the exclusions are deleted in the new rule. Thus, under the new rule, providers can send patients prescription refill reminders without an authorization regardless of whether a third party pays for or subsidizes the communication. A provider could also engage a business associate to assist it in distribution of these communications (6).

CAUTION: On the other hand, if a provider were to sell PHI to a third party, e.g., a list of patients with severe back pain to pharmaceutical manufacturer so that the manufacturer can send direct mail to the provider's patients to promote its products, that would be marketing

and would require a written authorization from the patient *before* the sale of the information occurs.

CAUTION: Although HIPAA allows a physician to recommend a product or service as part of the treatment of a patient or for case management or care coordination without it falling into the category of marketing, HHS notes that "such communication by a 'white coat' health care professional may violate the anti-kickback statute." (7).

Parents and Minors

Providers and parents had trouble with the old rule. Providers disliked it in that the language failed to assure that they could still use their own discretion to disclose information to parents when a state statute specifically gave them that discretion. Parents disliked it in that it prohibited their access to their children's records when state law would have allowed it (8).

The new rule carefully distinguishes between disclosure of records (providing PHI to persons or entities not employed by or training with the provider's practice) and access to records (a type of disclosure that is the right of an individual or his/her personal representative to review or obtain a copy of the individual's medical records) (9). The new rule is very complicated, but can be stated in these terms:

General Rule. If, under applicable law, a parent has authority to act on behalf of an unemancipated minor (e.g., under 18, not married) in making decisions related to health care, the provider must treat the parent as a personal representative with respect to PHI relevant to such personal representation.

Exceptions to the General Rule. A parent may not be the personal representative of an unemancipated minor, and the minor has the authority to act as the individual who is the subject of the PHI and to control access and disclosure of PHI, if:

(1) The minor consents to a particular health care service, no other consent to the health care service is required by law, and the minor has not requested that the parent be treated as the personal representative;
(2) The minor may lawfully obtain health care services without the consent of a parent, and the minor, a court, or another person authorized by law consents to the health care service in question; or
(3) A parent assents to a confidentiality agreement between the provider and the minor with respect to a particular health care service.

Exceptions Not Applicable. Notwithstanding any of the exceptions listed above:

(1) The provider may disclose or provide access to PHI about an unemancipated minor to a parent if applicable state case or statutory law or other applicable law explicitly permits or requires disclosure.
(2) The provider may not disclose or provide access to PHI about an unemancipated minor to a parent if applicable state case or statutory law or other applicable law explicitly prohibits disclosure.
(3) If applicable state case or statutory law or other applicable law is silent as to whether disclosure of PHI about an unemancipated minor is required, permitted, or prohibited to be made to a parent, then the provider may provide or deny access to PHI about an unemancipated minor to a parent if the parent is not a personal representative because one of the exceptions above applies and if allowing or denying such access is consistent with state case or statutory law or other applicable law, provided that the decision to allow or deny access must be made by a licensed health care professional in the exercise of professional judgment (10).

Providers should check with an attorney in their state regarding when to allow parents access to their children's medical records and when to disclose PHI about children to their parents.

PROTECTIONS AND ASSISTANCE FOR PROVIDERS

Incidental Disclosures

Many providers expressed concern that the old rule forbade any conversations concerning a patient's condition if there was any chance the conversation could be overheard. They also questioned whether they would continue to be permitted to use sign-in sheets in waiting rooms (11).

The new final rule allows uses and disclosures of PHI that are incidental to uses and disclosures permitted by the rule, subject to the "minimum necessary" requirement, i.e., a provider can only use or disclose the minimum

amount of PHI necessary to accomplish the purpose for which the use or disclosure was made, as well as the requirement that providers implement safeguards to keep unintended disclosures of PHI to a minimum. For example, a provider could instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room. Assuming the provider made reasonable efforts to avoid being overheard and reasonably limited the information shared, the incidental disclosure of PHI to patients in the waiting room is permissible under the new rule (12).

CAUTION: If you use sign-in sheets in your waiting room, you should limit the information on them as much as possible. Obviously, the safest sign-in sheet would just ask for a patient's name. DO NOT ask the patients to describe why they are presenting on the sign-in sheet.

Business Associate Contracts

The new final rule retains the requirement that physicians enter into written contracts with their business associates (vendors who need access to patients' PHI to perform tasks for providers) to ensure that the business associates will maintain patient privacy. Unlike the old final rule, the new final rule contains a model business associates contract that providers can and should use verbatim (13).

CAUTION: Keep in mind that the model business associates contract in the regulations does not have preamble and agreement language or signature blocks; these will need to be added if the provisions in the regulations are used as a stand-alone agreement as opposed to being incorporated into a new or an existing agreement describing the complete business relationship of the parties. Further, if the sample agreement is used as a stand-alone agreement, make sure to add a provision referring to the written contract that sets forth the business relationship of the parties and state that in the event of any conflict between the business relationship contract and the business associate agreement, the latter will control.

CAUTION: Business associates of large numbers of providers may have already drafted a business associate contract of their own for providers to sign that is extremely favorable to the business associate and may even leave out obligations of the business associate under HIPAA, that may require the provider to take on obligations not required under the rule, and that may leave out termination provisions required by the rule. These business associate agreements are usually presented to providers as an easy way to cross one business associate contract off their lists. Providers should ask their own attorneys to evaluate agreements presented to them by vendors against the business associate requirements of the new final rule.

CAUTION: Many simplistic overviews of the HIPAA rules have created confusion concerning the deadline for entering into business associate agreements. Here is a summary of the new final rule's requirements:

- If, prior to October 15, 2002, a provider entered and is operating pursuant to a written contract or other written arrangement with a business associate for the business associate to perform functions or activities or provide services that make the entity a business associate and the contract or arrangement is not modified or renewed from October 15, 2002 until April 14, 2003, then the contract or arrangement is deemed compliant with the new rule until the earlier of:
    - the date such contract or arrangement is renewed or modified on or after April 14, 2003, or
    - April 14, 2004.

During the deemed compliance period, the provider may disclose PHI to a business associate and may allow a business associate to create, receive, or use PHI on its behalf pursuant to a written contract or other written arrangement with such business associate. During the deemed compliance period, the provider still has a duty to comply with the new rule's requirements regarding an individual's right to copy and inspect PHI, amend PHI, receive an accounting of disclosures of PHI, and have the provider mitigate the harmful effects of improper disclosure of PHI with respect to PHI held by a business associate.

For business associate relationships entered into on and after October 15, 2002, a written contract must document the relationship and must contain business associate provisions in accordance with the new HIPAA Privacy Rule or, in the alternative, a separate written business associate agreement regarding the use and disclosure of PHI by the business associate must be finalized; such contracts must be in force no later than April 14, 2003 (14).

Realistically, does any physician practice have the time and the personnel resources to monitor these convoluted deadlines? Providers might save themselves some angst by having all their business associate contracts in place by April 14, 2003.

Research

The December 2000 rule required a special type of authorization for research that included treatment of individuals. Further, the old rule prohibited combining an authorization with any other legal permission related to a research study. Under the new final rule, researchers will need only one form for informed consent and authorization, and the requirement for a special type of authorization for research that includes treatment of individuals has been eliminated (15).

Authorizations

The old rule required multiple types of authorization forms. Under the new rule, only one type of authorization form need be used to obtain a patient's permission for a use or disclosure of PHI not otherwise permitted under the privacy rule. According to HHS, patients would still need to sign advance authorizations for each type of use or disclosure of PHI (e.g., marketing, research), but the provider would not need to use different types of forms.

Under the new rule, the minimum necessary rules do not apply to uses and disclosures of PHI made pursuant to a valid authorization signed by the patient (16). In addition, a provider does not have to keep track of disclosures of PHI made pursuant to a valid authorization for purposes of accounting to the patient for disclosures of PHI (17).

Limited Data Set

The new final rule adds a provision that allows providers to create and disclose a limited data set (that does not include individually identifiable health information) only for purposes of research, public health, and health care operations. However, a limited data set may be disclosed only if the provider who created it and the recipient enter into a data use agreement. In the data use agreement, the recipient must agree not to identify the information or use it to contact the individuals, among other things (18).

Accounting for Disclosures of Protected Health Information

Under the old rule, a patient could request an accounting of disclosures of PHI up to six years prior to the date of the request, and the provider would have to account for each release of PHI about the patient, except for releases to carry out treatment, payment, health care operations, and for certain other activities. The old rule did not have an exception for releases made pursuant to valid authorizations or for incidental disclosures or for disclosures made as part of a limited data set.

The new final rule clarifies that providers do not need to document or account for disclosures of PHI made pursuant to a valid authorization by the patient. Incidental disclosures and disclosures that are part of a limited data set also do not have to be documented or accounted for (19). The new rule also adds a provision allowing for a condensed accounting of disclosures of PHI related to research studies involving 50 or more individuals (20).

Sale of Practice

In the old rule, HHS unintentionally omitted from the definition of "health care operations" the transfer of PHI to the purchaser or successor in interest of a practice. If this had not been corrected, the new rule would have required an authorization from every patient of the practice to allow their PHI to be transferred to the purchaser or successor in interest. The new final rule clarifies that disclosures of PHI are allowed in certain circumstances when a provider is selling his or her practice, including the due diligence period (21).

Employment records

Many providers were confused under the old rule as to whether the employment records they keep for their own employees would be PHI under HIPAA. The new final rule clarifies that PHI does not include employment records (21).

Disclosures to another provider, a health plan, or a health care clearinghouse

The old rule restricted a provider's ability to share PHI with other covered entities (e.g., providers) if the disclosure was for the payment or health care operations purposes of the other covered entity. The new final rule

makes clear that providers can disclose PHI to other providers, health plans, and health care clearinghouses for the purposes of treatment and payment. For example, if a physician refers a patient to another provider and that provider calls and asks for information about the patient that s/he needs to file a claim, the physician does not need an authorization from the patient allowing him or her to disclose the information. Permitted disclosures of PHI to other providers, health plans, and health care clearinghouses for purposes other than treatment and payment are still limited (22).

Uses and Disclosures Regarding FDA-Regulated Products/Activities

The old rule allowed covered entities (including providers) to disclose PHI to a person or entity subject to the FDA's jurisdiction, but only for limited purposes. The new final rule allows providers to report to persons and entities that are subject to FDA jurisdiction concerning any information that is related to the quality, effectiveness and/or safety of the FDA-regulated product or activity for which the person or entity is responsible, e.g., adverse reactions (23).

CHANGES TO THE ELECTRONIC TRANSACTIONS STANDARDS

HHS published a proposed rule (24) on May 31, 2002 to change the Standards for Electronic Transactions, which were originally published in August, 2000 at (25). These standards will require providers who perform certain "standard transactions" electronically, such as filing claims, to follow certain formats and use certain code sets. The proposed changes to the transaction rule are limited and technical and include the following implementation specifications:

- Some data elements that were previously required will now be situational. For example, the data element "date last seen by physician", which is only needed by Medicare for certain physical therapy claims, will not be required for all claims but will be required on Medicare claims.
- Some data elements were removed because they were unnecessary. Examples include the estimated date of birth and a referral date.
- Certain items will be allowed to be reported with an external code set instead of a data element. For example, newborn birth weights and special program indicator codes will now be able to be reported via external code sets rather than making them data elements in the transaction.
- Several additional data elements, codes, and loops will be added to enable covered entities to perform certain business functions in transactions. For instance, providers and insurers can now cross-reference two subscriber IDs, e.g., surviving spouse and dependents.

NATIONAL STANDARD EMPLOYER IDENTIFIER

The Department for Health and Human Services published the final rule (26) on the employer identifier standard on May 31, 2002. The final rule provides that the Employer Identifier Number (EIN) must be used to identify employers. Health care plans, clearinghouses, and providers must use the EINs to identify employers in connection with electronic health transactions.

Requiring covered entities to use a standardized employer number is aimed at simplifying the administration of the health care system to enable efficient transmission of health information. For example, employers need to be identified when they transmit electronic information to health plans either to enroll or disenroll an employee as a participant. Employers also need to be identified when submitting premium payments.

Most employers already have an EIN if they pay wages to more than one employee. An EIN is assigned by the IRS, and can be obtained by filing a Form SS-4, Application for Employer Identifier Number, with the IRS. HHS stated the IRS agreed to the use of the EIN for health care purposes. Health care providers, health plans, and health care clearinghouses may obtain an EIN by asking the employer for the number.

NEW CHANGES IN DATA STANDARDS: PROPOSAL TO DROP THE NDC

A proposed rule to modify the standards for retail pharmacy transactions was announced on May 31, 2002 (27). The rule proposes to repeal the National Drug Codes (NDC) as the medical data code set for reporting drugs and biologics in all transactions, excluding retail pharmacy transactions, for which standards have been adopted.

The NDC was adopted as the standard originally because it is a unique number capable of identifying each drug or biological product. The adoption of the standard was

meant to aid in the efficiency and effectiveness of electronic transactions. Since the adoption of the final rule, however, the industry indicated standardization of the reporting of drugs and biologics using one coding system was not practical at this time. Several factors led to the proposal to drop the NDC, including:

- There was an overwhelming cost issue. The implementation of the NDC would require expansion of data field sizes in all physician practice management systems, so that displaying thousands of drug codes would be possible. Complete system re-engineering or replacement would have been required. Studies showed the cost to be immense, possibly exceeding an institution's costs for all other combined HIPAA-regulated compliance.
- The NDC is flawed, in that it shows how the drug was acquired, but it does not show the drug dosage.
- There was a systems incompatibility among institutional pharmacies, inpatient medical records and inpatient accounting systems that would require an expensive system re-tool and significant retraining of employees.
- Patient accounting systems do not accommodate the eleven digits of the NDC assignment.

The proposed rule provides a choice of two alternatives for the replacement of the NDC. The first choice is to not have a replacement at this time. The proposed rule notes that the benefit of not having a replacement code is the fact that HHS will have more time to fully evaluate the alternatives available. The other choice is to replace the NDC with the HCPCS for reporting drugs in nonretail pharmacy transactions. The benefit of adopting the HCPCS is that it is already in widespread use in the industry. Thus, the cost will be minimal to enact it as the replacement.

HIPAA press releases and Fact Sheets can be accessed at http://www.hhs.gov/ocr/hipaa

ACKNOWLEDGEMENTS

Ms. McMahon gratefully acknowledges the assistance of Sharon Gold, a summer associate, in researching and drafting this article.

REFERENCES

1. 45 CFR 164.520(c)(2).
2. 67 FR 53240.
3. 45 CFR 164.501.
4. 45 CFR 164.508(a)(3).
5. 67 FR 53186.
6. 67 FR 53187.
7. 67 FR 53188.
8. 67 FR 53200.
9. 67 FR 53200-01.
10. 45 CFR 164.502(g)(3).
11. *67* FR 53193.
12. 67 FR 53194.
13. 67 FR 53264.
14. 45 CFR 164.532(d)-(e).
15. 67 FR 53224-25.
16. 45 CFR 164.502(b)(2)(iii).
17. 45 CFR 164.528(a)(1)(iv).
18. 45 CFR 164.514(e).
19. 45 CFR 164.528(a)(1).
20. 45 CFR 164.528(b)(4).
21. 45 CFR 164.501.
22. 45 CFR 164.506(c).
23. 45 CFR 164.512(b)(1)(iii).
24. 67 FR 38050.
25. 65 FR 50312.
26. 67 FR 38009.
27. 67 FR 38044.