The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Pharmacy Benefit: Implications for Health Plans, PBMs, and Providers

DANIEL C. WALDEN, JD, and ROBERT P. CRAIG, PharmD

ABSTRACT

OBJECTIVE: To summarize and analyze the key provisions of the Health Insurance Portability and Accountability Act (HIPAA) and the impact on pharmacies, health plans, pharmacy benefit managers, and others involved in the delivery of pharmacy services and managed pharmacy benefits.

BACKGROUND: HIPAA was enacted by Congress in 1996 with the goals of administrative simplification in the health care system as well as protecting the privacy of individuals. HIPAA imposes new standards for health care transactions and patient privacy and defines new patient rights regarding their health care information. Transaction standards took effect October 16, 2002, while the privacy standards have a compliance date of April 14, 2003. Regulations, or “standards,” will apply to health plans, pharmacies, and other health care providers and other businesses involved in the delivery of health care services. Failure to comply will be punishable under the law. The U.S. Department of Health and Human Services estimated the 10-year cost of compliance to be $17.6 billion.

CONCLUSION: HIPAA’s new requirements will demand significant effort and expense for systems and business process development. Businesses from the smallest independent pharmacy to the largest health plans must be compliant by the deadlines imposed by HIPAA.

KEYWORDS: HIPAA, PBM, Regulation, Transaction, Patient privacy, Business associate, Covered entity

J Managed Care Pharm. 2003(9)1: 66-71

Understanding HIPAA’s Requirements and Deadlines

HIPAA required HHS to adopt standards in 8 specific areas. A summary of the standards required by HIPAA and the status of the rule-making process with respect to each is presented in Table 1.
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
and the Pharmacy Benefit: Implications for Health Plans, PBMs, and Providers

Changes Required for Compliance

The various standards adopted by HHS under HIPAA will have a significant and lasting impact on all organizations participating in the delivery of health care. This is not simply a matter of a few new regulations; rather, the HIPAA standards include a broad range of new obligations and requirements that will require extensive changes in systems, administrative procedures, and contracting practices. In many instances, compliance with the HIPAA standards will require organizations to develop capabilities they would otherwise not even have considered, and those developments will come at a great expense.

Transaction Standards

The most immediate change for the health care industry has been the need to develop systems able to use the formats and code sets specified in the transaction standards. Prior to the transaction standards, which took effect in October 2002, communications among doctors, hospitals, HMOs, insurance com-

| TABLE 1 | Summary of HIPAA Standards |
| --- | --- | --- |
| HIPAA Standard | Requirements | Compliance Date/Status |
| Electronic transactions (formats and code sets) | Defines 10 common information exchanges (each a transaction) between parties in health care (e.g., claims information, payment advice, eligibility). Specifies standard formats (e.g., NCPDP Version 5.1) to be used when those exchanges are communicated electronically and the code sets (e.g., National Drug Code) to be used to encode data elements. | For large covered entities: October 16, 2002 (a one-year extension is available to October 16, 2003, by submitting a plan to HHS for achieving compliance by the new deadline.) For small covered entities (fewer than 50 participants): October 16, 2003 |
| Privacy | Limits use and disclosures of individual health information, primarily to activities related to treatment, payment, and health care operations, and includes safeguards and restrictions regarding disclosure of records for public health, research, and law-enforcement purposes. Establishes additional patient rights, including giving patients access to their medical records. Restricts use or disclosure of health information to the minimum needed for the intended purpose. Adds significant administrative requirements. | For large covered entities: April 14, 2003 or small covered entities: April 14, 2004 |
| Security | Specifies the administrative procedures and physical means to ensure the confidentiality, integrity, and availability of protected health information. | Proposed standards first issued in 1998 have not been finalized. The compliance deadline will be 24 months after date of final adoption. |
| National employer identifier | Standardizes identifying numbers assigned to employers by health plans, using existing employer identification number (EIN) used by the IRS. | July 1, 2004 |
| National provider identifier | Creates a single ID system to identify hospitals, doctors, nursing homes, and health care providers when filing electronic claims. | Proposed standards have not been finalized. The compliance deadline will be 24 months after date of final adoption. |
| National health plan identifier | Creates a standard system for identifying health plans to make it easier for health care providers to conduct transactions with different health plans. | HHS has not yet proposed standards. The compliance deadline will be 24 months after date of final adoption. |
| National individual identifier | Would have created a standard unique identifier for individuals for use in health care transactions. | HHS has not proposed a standard and indications are that it will not. |
| Electronic signature standards | Creates standards for an acceptable signature in an electronic transaction that is the subject of the transaction standards. | Originally included as part of the 1998 security standards proposal. The prospect for a final standard is uncertain. The compliance deadline will be 24 months after date of final adoption. |

Note: This table was prepared from data available in December 2002.
panies, PBMs, and other participants in the care of patients were conducted in a series of privately determined formats, each requiring different information and often using different words or codes to describe the same condition or treatment protocol. The goal of the transaction standards is to require all parties to use specific required formats for certain classes of electronic transmissions, such as eligibility verifications, claims submissions to health plans by providers serving their members, and remittance advice back to providers.

In choosing those formats and code sets that would become the standards, HHS relies on existing organizations that have been engaged for many years in setting standards for various aspects of the health care delivery system based on industry consensus. In the area of pharmacy benefits, HHS designated the National Council for Prescription Drug Programs (NCPDP) as the Designated Standards Maintenance Organization and adopted the NCPDP telecommunication standard version 5.1 and batch standard version 1.0 (modified version 1.1) formats as the standard for pharmacy claims. In December 2001, Congress made available a one-year extension for providers and health plans. For pharmacies, this extension has provided only a limited respite, since a critical mass of payers, including a number of Medicaid plans, have converted or are intending to convert to the 5.1 standard and likely will stop accepting claims submissions in the earlier versions well before the extended deadline of October 2003.

**Privacy Standards**

HIPAA's privacy standards affect not only an organization's systems but also the entire way that an organization operates. Covered entities must undertake a number of administrative or procedural changes, including appointment of a chief privacy officer responsible for developing and implementing confidentiality policies and procedures; developing procedures to safeguard protected health information; training all members of its workforce to follow those procedures; and implementing processes to handle grievances, whistle-blower complaints, and sanctions for noncompliance by members of its workforce. In addition, health care organizations must comply with a set of newly created patients' rights established under the privacy standards. To address these, an organization must make arrangements to:

1. provide a Notice of Privacy Practices clearly explaining how organizations might use and disclose protected health information;
2. enable patients to request privacy protections;
3. allow patients to inspect and copy portions of their protected health information, known as the Designated Record Set (DRS);
4. develop a process for patients to request amendments to their DRS; and
5. provide, on request, an accounting of any disclosures of the individuals protected health information (PHI) made other than in the course of treatment, payment, or health care operations.

The privacy standards provide detailed descriptions of these rights, including mandatory language, time frames for responding, and record-keeping requirements. Since these are rights that did not previously exist, most involve the development of new capabilities and mechanisms.

Originally, a provider engaged in direct patient care, although not a health plan, was obligated to obtain written consent from an individual prior to using or disclosing information even to perform requested treatment, such as to dispense a prescription. In August 2002, HHS modified the privacy rule. The final rule requires the provider to use reasonable efforts to obtain acknowledgment that the individual received the provider's Notice of Privacy Practices but no longer prohibits services from being rendered in the absence of formal written consent from the patient.

The central feature of the privacy standards is the provision that PHI, essentially identifiable health information held by a covered entity, may be used or disclosed by a covered entity only for purposes specifically approved in the standards. These limitations apply not just to the disclosure of information to third parties (the concern we have traditionally considered confidentiality) but also to uses or disclosures of information within an organization.

HHS clearly contemplated, however, the legitimate uses of health care information to effectively deliver health care services and protect the public. The standards therefore provide that PHI may be used for purposes of treatment, payment, or health care operations as well as to meet a number of public policy purposes such as responding to requests for information from law enforcement or the Secretary of HHS. In using information for payment or health care operations, a covered entity must make reasonable efforts to use the minimum amount necessary to achieve the intended purpose.

Finally, under the privacy standards, it is the responsibility of the covered entity, including a health care payer, to ensure that its business associates, such as PBMs, perform services in a manner consistent with the applicable HIPAA standards. It is important to note that the HIPAA privacy standards establish minimum standards for compliance nationwide. States may have more stringent privacy rules than those established under HIPAA. In those instances, a health care organization is required to follow the state rules. HIPAA privacy standards represent the floor for compliance, not the ceiling.

**Other Standards**

The standards that address transactions and privacy no doubt require the most sweeping changes of all the standards mandated by HIPAA. Covered entities must anticipate, however, the potential impact of the security and other standards. First proposed in 1998, HHS has not yet issued final security standards, and covered entities will have 24 months after the effective date in which to assure compliance. On the other
hand, certain capabilities required under the security standards are building blocks for compliance with the privacy standards. For instance, to effectively meet the requirement to make reasonable efforts to only use or disclose the minimum amount of information needed for a HIPAA-approved purpose, a company must have an effective way to control access by individuals to PHI within their organizations, an issue HHS has addressed in the proposed security standards. A covered entity taking guidance from the proposed security standards in developing its systems and processes for the utilization of data will be well ahead when the standards are finally adopted.

In May 2002, HHS adopted the standard for health plan identifier, essentially selecting the federal employer tax ID number already assigned by the Internal Revenue Service to be the identifier used when submitting an electronic transmission subject to one of the transaction standards. HHS is expected to adopt single identifiers for health plans and providers. HIPAA originally required HHS to adopt an identifier for individuals, but this is a highly controversial proposition opposed by many privacy advocates, and it has been set aside.

Consequences of Noncompliance With HIPAA

Health plans, pharmacies, and others directly subject to HIPAA are required to comply with the regulations by the specified deadlines, except where extensions have been granted. HHS has named its Office for Civil Rights to enforce the privacy standards and the Centers for Medicare and Medicaid Services (CMS) to enforce the transaction and code set standards. Penalties for violations of the HIPAA standards are $100 per violation, with an annual limit of $25,000 for violations of an identical requirement. Certain offenses relating to misuse or disclosure of individually identifiable health information carry penalties of up to $50,000 and imprisonment for not more than 1 year, with offenses "committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm" carrying penalties of up to $250,000 and imprisonment for not more than 10 years.

Although business associates are not directly subject to HIPAA or its penalty provisions, HIPAA requires that the covered entity cause its business associate to comply with the standards and, in fact, the privacy rule requires a business associate contract containing provisions that assure the business associate is compliant with the privacy rule and other aspects of HIPAA. Failure by business associates to comply, therefore, would expose them to the risk of contract termination with the covered entity (health plan sponsor) or loss of business at the very least. Companies such as PBMs, which serve in different business lines as business associates of covered entities, directly subject to HIPAA, may face greater risk of enforcement than companies that only act as business associates.

Implications for Pharmacy and the Pharmacy Benefit

While all health care organizations will be affected by the sweeping changes required by HIPAA, the various industries within health care, such as hospitals, physicians, and dental providers, will have to develop different approaches to meet the challenges, depending on their existing practices. The following describes how HIPAA applies to pharmacy and the pharmacy benefit, listing some of the issues and interpretations of specific note.

Pharmacies

Pharmacies are health care providers that are directly regulated as a “covered entity” subject to HIPAA. The pharmacy, whether a community, mail, or specialty pharmacy, is obligated to meet all of the HIPAA standards summarized above.

Under the transaction standards, the pharmacy must be prepared to submit claims in the NCPDP version 5.1 or batch 1.0 format and receive payment advice in Accredited Standards Committee X12 837. The requirement took effect on October 16, 2002, although Congress provided that covered entities that filed an extension could continue to use older formats for up to an additional year and still be in compliance with the law. Even among those pharmacies that filed for extensions, most have already expended substantial time and resources preparing to migrate to the new standards and will likely want to convert as soon as they are able, well before the one-year maximum extension.

Under the privacy standards, pharmacies must meet all of the new administrative requirements, including appointing their chief privacy officer, developing policies and procedures, and training their workforce in privacy procedures. They must also accommodate the 5 new patient rights. As noted above, under the final privacy rule, providers, including pharmacies, are no longer required to obtain written consent from an individual prior to using or disclosing information but must use reasonable efforts to obtain acknowledgment that the individual received the pharmacy’s Notice of Privacy Practices.

Pharmacies may use and disclose PHI to the extent specifically permitted under the privacy rule, and, of course, much of the activity undertaken by a dispensing pharmacy fits clearly within HIPAA’s definition of treatment. Other functions undertaken by a pharmacy may fit within the definitions of payment or health care operations.

For activities permitted under the privacy rule (other than those fitting the definition of treatment that are exempt from this requirement), pharmacies are required to use reasonable efforts to insure that any use or disclosure of or request for PHI involves the minimum amount necessary. This clearly requires a pharmacy to look at its internal operations, packaging, and customer service policies to determine that information not needed to complete a transaction is not used or disclosed. For example, the information included on the outside of a prescription label, itself, involves pharmacy practice, a treatment activity not subject to the minimum-necessary requirement, and the drug name may be included.
The minimum-necessary requirement applicable to providers in the context of claims submission has been a source of considerable discussion within the industry. Health plans that are asked to approve and pay claims are entitled to ask for information they believe is needed to conduct their functions. Such plans are covered entities that have a specific obligation to apply the minimum-necessary standard before making a request for information, and HHS specifically allows a provider to rely on the request of another covered entity. A pharmacy may, therefore, provide information required by health plans or their PBMs acting as business associates, without liability under the HIPAA privacy rule. Ultimately, the health plan determines what information is needed from providers to authorize payment and to conduct other aspects of their health care operations.

Health Plans

A second type of covered entity directly regulated under the HIPAA standards is the “health plan.” A health plan is defined as “an individual or group plan that provides or pays the cost of medical care.” The rule provides a nonexclusive list of the types of payers for health services covered by the rule, specifically including insurers, BlueCross BlueShield plans, health maintenance organizations, Medicare and Medicaid, and a number of other government programs. Employee welfare benefit plans are also health plans that are covered entities directly subject to HIPAA (the employer who sponsors an ERISA plan is not a health plan subject to HIPAA, but its health plan is and must meet specific requirements prior to allowing the plan sponsor access to PHI). Since more than 90% of drug spend in America today is covered at least in part by a third party, there will generally be a health plan with HIPAA obligations involved in most pharmacy activities.

As with providers, health plans, including insurers, health maintenance organizations, and ERISA plans, have direct responsibility to meet the HIPAA privacy requirements, providing to individuals the protections and rights under the HIPAA standards and having in place a privacy officer and other administrative requirements. Some requirements will be virtually impossible for many health plans to meet without assistance. For instance, the transaction standards require that the health plan accept claims from pharmacy providers in the “standard” format (NCPDP 5.1), but a plan typically does not contract directly with pharmacies or communicate with them directly. Rather, most health plans retain a PBM or other administrator to manage the network. The administrator would be a business associate of the health plan and may accept claims or submit payment advice in standard formats on the health plan’s behalf.

Health plans may use, disclose, or request PHI for treatment, payment, or health care operations, and may retain business associates to perform these functions. The activities involved in the administration of the drug benefit fall within these definitions. Health plans may use or disclose data for financial, actuarial, and clinical purposes. These functions may include analyses of utilization behavior, financial metrics related to plan performance, or performance of actuarial modeling. Other health care operations may include member and provider fraud and abuse surveillance, retrospective drug utilization review activities, disease and case management, and formulary administration.

Pharmacy Benefit Managers

A health plan may retain a “business associate” to perform functions the health plan would be permitted to perform under HIPAA. For instance, a health plan that offers a retail pharmacy benefit may retain a PBM to manage the pharmacy network and adjudicate claims. In this context, the PBM acts as a business associate of the health plan; it is not a business associate of the pharmacies in its networks.

Acting as a business associate, PBMs offer a broad array of services to health plans. It is useful to think of health plans in 2 groups. One group consists of plan sponsors that are primarily the final payers for the benefit, such as the ERISA plans sponsored by self-insuring employers. These clients tend to be engaged in their core businesses, such as auto manufacturing or financial services, unrelated to health care, and are unlikely to have the capabilities needed to meet HIPAA requirements. They are likely to require from PBMs a broader range of services to meet their HIPAA obligations. For instance, an employer-sponsored health plan may not have customer-service capabilities to accommodate a patient’s request for health care information and, therefore, may turn this request back to its PBM.

The second type of health plan consists of clients that are part of the health care delivery system, including HMOs and insurers. These and other participants in health care delivery will likely develop the internal capabilities needed to comply with HIPAA’s new requirements. In fact, they will, in turn, often serve as business associates of other payers, such as employers. For these, PBMs need to offer more robust capabilities to support the health plans’ systems. For instance, the PBM may provide regular data transmissions for use by the client’s customer-service staff. For either type of health plan client, PBMs must be fully prepared to meet the HIPAA standards by the respective deadlines.

First, a PBM must have made substantial investments of money and resources preparing to migrate from older NCPDP versions such as 3.2 and 4.1 to the new NCPDP version 5.1 standard by October 16, 2002. The legal responsibility to conduct transactions in compliance with the standards rests with the health plans, not the PBMs. The health plans look to their business associates—the PBMs—to meet the requirements on their behalf. If a PBM was not ready, therefore, all of the health plan clients would be out of compliance with the transaction standards. Because the extension was not available to a business associate, all of a PBM’s clients would have been required to file for an extension. The one-year extension legally available to retail pharmacies was of no practical use to the PBMs or their health plan clients.

Second, a PBM must have made the extensive changes in systems and organization required to establish the new admin
administrative controls. They must have appointed a privacy officer, conducted gap assessments, developed new policies and procedures, and trained their workforce. They must have entered into appropriate agreements with their vendors to meet the development associate requirement.

Third, a PBM must have the capability to assist the client in making available the 5 patient rights.

Fourth, the PBM must assure that the programs it operates as a business associate of its health plan clients are permitted under HIPAA. As noted in discussing the impact of the privacy rule on health plans, the activities of PBMs in managing the prescription benefit generally fit within the definitions of treatment, payment, or health care operations. The PBM must review its programs and services to assure that the specifics of each are consistent with the privacy rule and are operated consistent with the transactions and other standards where applicable.

Of course, some PBMs have mail and specialty pharmacy subsidiaries that are providers and are “covered entities” under HIPAA and must comply with all of the applicable requirements.

Conclusion

Everyone impacted by HIPAA faces significant effort to achieve compliance. Each of the key participants in the delivery of a funded drug benefit, including pharmacies, the health plans that pay for the benefit, and the PBMs they may retain, has specific obligations under HIPAA. In addition to the direct penalties under the statute, they risk breaching the terms of their business associate agreements and face client or customer loss.

Health plans that retain a PBM must, of course, exercise care and perform a level of due diligence, but, in the end, it is the PBMs themselves that can develop and implement the needed policies and practices. Similarly, managed care organizations and PBMs engaged in managing pharmacy networks must ensure that pharmacies will meet their responsibilities.

Health plans, their business associates, and pharmacies will be working diligently to complete the development work necessary to comply with all of the privacy standards by the April 14, 2003, deadline. At the same time, stakeholders should also be monitoring the finalization of remaining standards and any changes in the newly adopted privacy standards.

Notwithstanding the hundreds of pages of regulations, the HHS preamble to its proposed and final rules, official guidelines, and FAQs issued by HHS, not to mention the thousands of pages of legal analysis, there remains a good deal of ambiguity in what would be appropriate compliance with the various HIPAA standards. The roles of different participants and the specifics of compliance continue to be defined. What is certain, however, is that HIPAA is the law, it is not going away, and compliance is not optional.

REFERENCES

2. Id. Section 261. Purpose.
3. Id. Section 264. Recommendations with Respect to Privacy of Certain Health Information.
11. Ibid., at page 4. HHS and Congress have put development on hold, and since 1999, Congress has adopted budget language to assure no standard is developed without congressional approval.
12. Although the original proposed electronic signature standard was included together with the proposed security standard (see note 7, above), the subject matter is quite distinct. When the final security rule is published, it may not address electronic signatures.
14. See note 5 above.
16. 45 C.F.R. 164.320.
17. 45 C.F.R. 164.522.
18. 45 C.F.R. 164.224.
19. 45 C.F.R. 164.326.
20. 45 C.F.R. 164.528.
22. E.g., 65 FR at 82471-82472.
23. 45 C.F.R. 164.502 (a)(1)(ii) and 45 C.F.R. 164.506.
24. 45 C.F.R. 164.512.
25. 45 C.F.R. 164.502(b).
26. 45 C.F.R. 164.504(c).
27. 45 C.F.R. 160.203.
28. Public Law 104-191 Sec. 1176.
29. Id. Sec. 1177.
30. 45 C.F.R. 164.520(c)(2)(ii).
33. 45 C.F.R. 160.103.

ADDITIONAL RESOURCES

Further information can be found at the official federal HIPAA Web site at http://aspe.hhs.gov/admsimpl.

No outside funding supported this study. Author Robert P. Craig served as principal author of the study. Study concept and design and drafting of the manuscript was the work of Craig and author Daniel C. Walden. Analysis and interpretation of data was contributed by Walden.