

An Overview of
HIPAA

The Role of CPAs in
Privacy Compliance



Copyright ©2005 by
American Institute of Certified Public Accountants, Inc.
New York, NY 10036-8775

All rights reserved. Checklists and sample documents contained herein may be reproduced and distributed as part of professional services or within the context of professional practice, provided that reproduced materials are not in any way directly offered for sale or profit. For information about permission to copy any part of this work for redistribution or inclusion in another document or manuscript, please call the AICPA Copyright Permissions Hotline at (201) 938-3245. A Permissions Request Form for e-mailing requests is available at www.aicpa.org by clicking on the copyright notice on any page. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881.

1234567890 MI 098765

Complying With HIPAA

Opportunities exist for CPAs to assist health care organizations and providers in complying with the Health Insurance Portability Accountability Act (HIPAA) (Public Law 104-191). The privacy provisions of HIPAA affect all segments of the health care industry, requiring covered entities (see the discussion in the following sections) to use standard formats for many electronic transmissions of health data and to take specific measures to ensure the security and privacy of personal health information. Although the privacy provisions of HIPAA are already in place, this guide will help CPAs ensure that their clients continue to be in compliance with HIPAA.

Transactions

Health care entities that send common health care transactions by electronic means, such as claims, eligibility and claims inquiries, or enrollment and disenrollment records, must use certain standard electronic file formats and standard code sets designated by the regulations. For most entities, the compliance date for electronic transaction standards was **October 16, 2003**.

Security

The Security Standards rule adopts national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. HIPAA mandated security standards to protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. The Security Rule requires that covered entities develop, implement, and maintain appropriate measures to safeguard information. For most entities, the compliance date for security standards is **April 21, 2005**. Further information on this rule can be found at

<http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf>

Privacy

The privacy rule of the HIPAA regulation went into effect on **April 14, 2003**. The HIPAA privacy rule provides patients access to their medical records, control over how their health information is used and disclosed, avenues for recourse if their medical privacy is compromised, and a number of other privacy rights. Covered entities must have in place various processes to support and administer those rights.

Who Is Affected?

The rules protect patients' medical records and other personal health information maintained by the following covered entities:

- Health plans — Individual or group health plans offered by health maintenance organizations and health insurers, as well as employee health benefit plans offered by employers that provide or pay the cost of medical care.
- Health care providers — Providers of medical or health services and any person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business and sends common health care transactions, such as claims, by electronic means.
- Health care clearinghouses — Entities that process or facilitate the processing of nonstandard health information data elements and formats into standard data elements and electronic formats.

Leveraging their skills in understanding and examining information flows within organizations as well as assessing internal controls and processes for the systems that contain information, CPAs can turn the regulatory burden of the HIPAA privacy rule into an opportunity for health care providers to show not only that they comply with the rule, but also that they follow sound privacy practices.

Covered Entities and Individuals Both Have Privacy Obligations and Rights

The HIPAA privacy rule also defines some rights and obligations for both covered entities and individual patients and health plan members. Some of the highlights are:

- Individuals must give specific authorization before health care providers can use or disclose protected information in most nonroutine circumstances, such as releasing information to an employer or for use in marketing activities.
- Covered entities will need to provide individuals with written notice of their privacy practices and patients' privacy rights. The notice will contain information that could be useful to individuals choosing a health plan, doctor, or other provider. Patients will generally be asked to sign or otherwise acknowledge receipt of the privacy notice.
- Covered entities must obtain an individual's specific authorization before sending them marketing materials.

HIPAA requires health care organizations and providers to meet certain privacy standards with respect to personal health information. The HIPAA privacy rule specifically states that "a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The protection given must be for both intentional and unintentional disclosures of personal health information.

So What's Next?

The following checklist, *An Overview of HIPAA: Compliance and the Information-Handling Practices of Health Care Organizations and Providers*, is designed for use by CPAs to assist their clients in complying with the HIPAA privacy rule. It provides a targeted look at some of the issues facing small to medium-size health care providers in complying with the privacy provisions of HIPAA. This checklist should be used to alert CPAs and their clients to areas in which their compliance effort may fall short. This will help CPAs perform a gap analysis and identify priority areas for advisory work.

HIPAA is multifaceted, covering many areas of personal health information. This questionnaire focuses only on the privacy provisions of HIPAA and is not intended to cover all matters that need to be considered in order to comply with all of the requirements of HIPAA. CPAs can add tremendous value to their clients in helping them design effective privacy programs and follow solid privacy practices.

An Overview of HIPAA: Compliance and the Information-Handling Practices of Health Care Organizations and Providers

This checklist provides an overview of the key information practice areas covered under the Health Insurance Portability Accountability Act (HIPAA) for which small to medium-size health care organizations and providers must be in compliance with. This checklist focuses on HIPAA privacy provisions and is not intended to cover all matters related to overall HIPAA compliance. Following are questions associated with the fair information practice areas that are key to the proper management of personal information and are consistent with the AICPA/Canadian Institute of Chartered Accountants Privacy Framework.

CPAs should discuss these topics with the organization and collect documentation or observe processes in place as the issues are discussed. A response of "No" could indicate a gap in the HIPAA compliance process. A response of "Yes" could indicate some level of HIPAA preparedness but does not ensure that all privacy-related details have been appropriately addressed for HIPAA compliance. This checklist should be used to alert health care organizations and practices to areas in which they may require further preparation related to the privacy provisions of HIPAA. Before completing this checklist, CPAs are advised to understand the HIPAA privacy and administrative simplification provisions and their impact on the operations of a health care organization or providers.

For the purposes of this document, the term protected health information (PHI) includes essentially all information a provider has that is personally identifiable information (that is, any information relating to an identified or identifiable individual, including written, spoken, and electronic information).

Questions for the Organization	Yes/No or N/A	Comments
Privacy Program		
1. Do you have a designated privacy official to oversee your privacy program?		
2. Are your company's privacy policies and procedures documented in writing?		
3. Do you have a general policy on privacy of individual health information?		
4. Have you undertaken or reviewed an analysis of preemption issues and possible interactions between HIPAA and state privacy laws?		
Notice and Purpose		
5. Do you provide a dated notice of privacy policies and practices written in plain language to patients regarding their privacy rights?		
6. Does the notice describe the use and disclosure of PHI that may be made without the patient's specific authorization?		
7. Does the notice describe the uses and disclosures you may make that are permitted and/or required by law?		
8. Does the notice state that other uses and disclosures will be made only with the patient's authorization?		
9. Does the notice state that a patient can inspect, copy, or amend PHI (subject to specific procedures), and receive an accounting of disclosures of PHI by the practice?		
10. Does the notice state that the organization may change or revise its privacy policy at any time and that patients will be informed of significant changes?		
11. Does the notice indicate the patient can complain to the organization, and does it include contact information for complaints?		

Questions for the Organization	Yes/No or N/A	Comments
Choice and Authorization		
12. Do you obtain authorizations from individuals for the use or disclosure of their PHI for reasons other than treatment, payment, or health care operations?		
13. Do you obtain authorization when a patient requests disclosure of his or her own PHI?		
14. Does the authorization identify the individual or class of individuals to whom the information will be disclosed?		
15. Does the authorization describe the kind of information to be disclosed?		
16. Does the authorization include some kind of date or event upon which the authorization will terminate?		
17. Does the authorization form clearly indicate the patient has the right to revoke the authorization?		
18. Do your privacy policies recognize the authority of the properly designated personal representative of an individual to act on behalf of the individual in matters pertaining to privacy rights and control of PHI?		
19. Do you have a process for receiving and evaluating requests from individuals to restrict further use or disclosure of their PHI for purposes of treatment payment or health care operations?		
20. Do you have a process for receiving and evaluating requests from individuals to receive communications of their PHI by alternative means or at alternate locations?		

Questions for the Organization	Yes/No or N/A	Comments
Use and Retention		
21. Do you have a policy and procedure covering use and disclosure of PHI for public health activities, judicial proceedings, and law enforcement purposes, or covering disclosure to coroners, medical examiners, or funeral directors?		
22. Do you have an established procedure to verify the identity and authority of persons requesting PHI?		
23. Do you have protocols specifying the minimum amount of information needed for frequent, routine disclosures of PHI?		
24. Do you have policies and procedures, including written criteria, for determining the minimum amount of information needed for nonroutine disclosures of PHI?		
25. Have you defined and documented your organization's designated record set(s)?		
26. Do you have a document retention policy that specifies a retention period of six years for documentation required by the privacy rule?		
Access		
27. Is there a policy and procedure related to how a patient can request access to his or her own PHI?		
28. Have you identified the locations of records in the designated record set(s), and developed a process for collecting such records to fulfill an individual's request for access?		
29. Does your procedure include a process for denying access to records containing PHI in certain circumstances, and include a right to review of the denial in some cases?		
30. Have you determined how you will provide copies of the information if requested by the individual?		
31. Do you have a process and procedure to address requests for amendment of incorrect PHI?		
32. If a request for amendment is accepted, do you have a process to make the appropriate modifications and make reasonable efforts to notify others that have previously received the incorrect PHI?		
33. If the request for modification is denied, do you have a process to clearly notify the patient of the reason for the denial and that a written statement of disagreement may be prepared by the patient and filed with the denial, and describe the complaint procedures, including contact information?		

Questions for the Organization	Yes/No or N/A	Comments
Security		
34. Do you have processes in place to limit access to PHI only to those in your organization who have a need to access the information for authorized purposes?		
35. Do you have processes in place to mitigate any harmful effect of the use or disclosure of PHI?		
36. Do you have administrative, technical, and physical safeguards in place to protect the privacy and security of PHI in all forms?		
37. Have you implemented processes to ensure other patients do not inadvertently see patient names, charts, fee slips, lab results, or other PHI?		
38. Have you implemented reasonable safeguards to protect patient privacy? For example, has your staff been trained to lower their voices when discussing patient-specific information when within hearing of others outside the organization, such as other patients, or to move to another area where they cannot be overheard? Refer to additional guidance prescribed by the Office for Civil Rights (OCR) www.hhs.gov/ocr/hipaa/privacy.html		
39. Are your systems for storing physical records containing PHI secure and reasonably inaccessible to non-employees?		
40. Do you use workstation controls on computer terminals, such as passwords, automatic timed logoff, and screen savers?		
41. Has the security of your computer system been reviewed by someone with appropriate skills to determine if appropriate security is in place to prevent unauthorized access to PHI?		

Questions for the Organization	Yes/No or N/A	Comments
Onward Transfer and Disclosure		
42. Have you identified all contractors or vendors to whom you disclose PHI and who use PHI to perform a service or function for you or on your behalf? Do you have business associate agreements in place with all such vendors and contractors?		
43. Does each business associate agreement contain all of the provisions required by the privacy regulations?		
44. Do you have a system in place to document when and to whom PHI has been disclosed?		
45. Are the kinds of information being disclosed and the purpose of the disclosures documented?		
46. Are copies of requests for disclosure retained?		
47. Do you have a policy and procedure for providing an accounting of disclosures to the individual on request?		
48. Is this documentation of disclosure included in your document retention policy? (It must be retained for a minimum of six years.)		
49. Do you have a process for determining whether and when de-identified data can and should be used?		
50. Do you have an established method for de-identifying PHI?		
51. Has the method for de-identifying PHI been tested?		
Management and Enforcement		
52. Do you have a training program to educate your employees on HIPAA and your company's privacy policies and procedures?		
53. How is the training provided?		
54. How often do you conduct employee privacy training?		
55. How do you document employees' completion of this training?		
56. Do you have a policy and process to discipline employees who do not comply with your privacy policies and procedures?		
57. Do you have a process for mitigating and controlling the effects of inappropriate disclosures of PHI?		
58. Have you designated a contact person or office responsible for receiving complaints and providing further information?		

NOTE: You should also ask your clients how they comply with HIPAA's electronic transaction standards and other administrative simplification provisions. This may include asking them if they electronically transmit transactions and other data in accordance with designated American National Standards Institute (ANSI) and National Council for Prescription Drugs Program (NCPDP) standards.



For more information

To learn more about privacy and how implementing new privacy measures can benefit your organization, please visit www.aicpa.org/privacy

