MIEC

SPECIAL REPORT

MIEC Claims Alert

Number 34
Revised 2008

HIPAA's Privacy Act: A compliance primer for the solo and small group practice

INSIDE

Special Report Claims Alert

A publication of the Loss Prevention Department, Medical Insurance Exchange of California, 6250 Claremont Ave, Oakland, CA 94618. Articles do not constitute legal advice.

This newsletter addresses one of the most significant components of the multi-faceted Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations: the Privacy Act. The Privacy Act has been finalized and those who must comply with it must do so by April 14, 2003. The Privacy Act was written to give patients more control over their medical information; to set boundaries and establish safeguards on the release of Protected Health Information (PHI); to hold violators accountable for breaches of privacy; and to strike a balance between the right to individual privacy and the necessity for disclosure to protect public health.

Many physicians are concerned about what the Privacy Act really means to their practices and what they will have to do to comply. The most time-consuming aspect of the Privacy Act will be its initial implementation; once the components of the Act are well-established, their upkeep will probably be minimal, and may be similar to the policies most physicians already practice to preserve patient confidentiality. This article will outline the fundamentals of what physicians in solo or small group practice must do to comply with the Privacy Act. (Large multi-physician and multi-specialty group practices and clinics will need to rely on training and advice by carefully-selected professionals dedicated to the nuances of HIPAA compliance in such practices.) It also directs those physicians to additional resources to assist in "fine tuning" the execution of the basic requirements. The Privacy Act is intended to encourage physicians to do that which is *reasonable* and *appropriate* to protect patients' privacy and confidentiality.

In short, the Privacy Act requires: (1) that patients be educated about privacy protection; (2) a written privacy policy; (3) a designated privacy officer; (4) employee training in privacy policies; (5) that patients have access to their PHI; (6) that patients may request amendments to their PHI; (7) that patients must sign an authorization to disclose PHI for nonroutine uses not otherwise permitted or required; and, (8) that patients may obtain a history of nonroutine disclosures made after implementation of the Privacy Act. This newsletter will not answer all your questions. It will summarize the fundamentals of the Privacy Act, and it will end with a list of resources that offer more detailed and comprehensive information for little or no cost.

The first concern: Who must comply with the Privacy Act?

Covered entities

Although many individual licensed healthcare providers and organizations qualify as "covered entities (CE)," this article will address the requirements of physicians who are covered entities; throughout the

remainder of this newsletter, the word "physician" will refer to those physicians who meet the following criteria as a covered entity.

Physicians must comply with HIPAA's Privacy Act if they transmit, or someone transmits on their behalf, PHI in electronic form to accomplish at least one of the following:

- Submit health care claims;
- Coordinate benefits;
- Confirm health care claim status;
- Facilitate health care payment and related advice;
- Enroll or disenroll in a health plan;
- Confirm eligibility for a health plan;
- Arrange for health plan premium payments;
- Obtain referral certification and authorization;
- File a first report of injury;
- Send health claims attachments; and
- Transact other business that the Secretary of Health and Human Services (HHS) may prescribe by regulation.

Protected health information (PHI) is individually-identifiable documentation of mental or physical medical conditions, the treatment of those conditions and the payment for that care. In other words, PHI is confidential patient information.

Physicians are exempt from the HIPAA standards if they do not, nor does anyone on their behalf, submit electronically any of the transactions described above; they submit **only** paper forms to third-party payers; and/or they do not accept Medicare patients. (Faxed information does not fall into the "electronic transaction" category.)

Physicians who accept Medicare patients automatically qualify as CE because beginning in October 2003, Medicare will accept only electronically submitted claims. Physicians' offices with fewer than 10 full-time employees may be exempt from this mandate; however, exemption is not automatic, and the Centers for Medicare and Medicaid Services (CMS) has yet to publish the process by which exemptions will be granted. If a billing service submits electronic transactions on behalf of a physician practice with fewer than 10 full-time employees, that practice must nonetheless comply with HIPAA.

Preparing to comply

Many already-compliant physicians and their office staff began by assessing their current privacy policies. Several useful and user-friendly self-evaluation privacy policy checklists or questionnaires are available on the Internet at no cost to the user. A few examples of questions to be considered include: Where do we leave charts; are they in places where other patients might see them? Who sees patients' confidential information in the course of business? How closely do we monitor our conversations when patients are within earshot? How do we protect our computer security? How do we maintain awareness of what we say on the telephone in patients' presence? With what frequency do we update our virus detection software? What is the process by which departing employees return keys, cards, or other significant office property? The purpose of the assessment is to identify gaps in current policy that might jeopardize patient confidentiality.

Glossary of HIPAA terms

BA	Business Associate
CE	Covered Entity
CMS	Centers for Medicare and Medicaid Services (formerly known as HCFA)
HHS	Health & Human Services
PHI	Protected Health Information
TPO	Treatment, Payment, Operations

Another helpful preparation for Privacy Act compliance is to review state law, because contrary and more stringent state law will prevail over the HIPAA standards. A privacy officer should be appointed; in larger practices, a committee to assist the privacy officer would be appropriate. The physician and office manager should alert the staff to the heightened awareness of confidentiality, ask all to consider what should be included in a privacy policy, review current state law and document preparatory education and activities that lead to Privacy Act compliance.

The compliant office will have the following basic privacy documents: (1) an Authorization form for the nonroutine release of PHI; (2) a Notice of Privacy Practices; (3) a Privacy Policy; and (4) an agreement for Business Associates (BA) to sign, all of which are described below.

Treatment, Payment and Operations (TPO)

Patients will not be required to sign a general consent for

disclosure of their PHI in the interest of what the Privacy Act calls Treatment, Payment and Operations (TPO). "Treatment" refers to communications related to the provision, coordination, and management of health care and related services. This includes, but is not limited to, coordination with co-treaters, consultation between providers, and referrals to providers.

There is no limitation to communication of PHI between these entities for treatment purposes which necessitate full disclosure.

"Payment," the second component of TPO, refers to those transactions required to obtain reimbursement for health care services, including but not limited to: determining eligibility, billing claims management, medical necessity review, utilization review, etc.

The term "Operations" includes a wide variety of business activities essential to the ongoing management of a medical office practice, such as (but not limited to): quality improvement, performance evaluations, training programs, licensing, credentialing, medical review, professional liability services, legal services, auditing, etc.

Physicians do **not** need to obtain written consent from their patients for routine disclosures of PHI in the interest and pursuit of Treatment, Payment and Operations. Once again, there is no limitation to disclosure for treatment purposes. However, physicians are required by the Privacy Act to make reasonable efforts to use or disclose the "minimum amount of confidential information necessary" to accomplish Payment and Operations.

Psychotherapy notes exception

Much of a psychiatrist's patient chart may be released for purposes of TPO, including the following: medication orders and monitoring; counseling session start and stop times; modalities and frequencies of treatment; clinical test results; and summaries of diagnoses, functional status, the treatment plan, symptoms, prognosis, and patients' progress. *However*, what are commonly known as "process notes," or psychiatrists' private notes that document or analyze counseling session content and are separate from patients' medical record, are additionally protected. Patients do not have the right to inspect or copy these notes and separate authorization is required for their release, even for TPO.

Authorization for nonroutine disclosures

For nonroutine, non-TPO-related disclosures, physicians must obtain patients' written authorization. Criteria for this authorization are mandated by the HIPAA Privacy Act, and physicians are prohibited from using this authorization as a provision of treatment. The authorization form itself must be written in plain language and must include:

- The name of the persons who are authorized to release the PHI;
- The name of the persons to whom the PHI will be disclosed;
- A description of how the PHI will be used;
- An explanation that the authorization may be revoked, unless the original authorization has already been relied upon;
- An explanation of how the authorization may be revoked;
- An expiration date for the authorization; and
- The patient's signature.

The physician must keep a copy of this authorization. We suggest that the patient be given or offered a copy of the signed form.

Exceptions to disclosure for TPO and the need for authorization

The Privacy Act names some exceptions, circumstances in which a physician may disclose PHI, that do not fall into the categories of TPO and do not require patient authorization for disclosure. These include:

- State reporting requirements, such as the duty to warn individuals of imminent danger from a patient, child or elder abuse, domestic violence, neglect, etc.;
- State requirements for the release of information related to Workers Compensation claims;
- Public health activities;
- Health oversight activities;
- Judicial and administrative proceedings;
- Criminal investigation by law enforcement officials;
- Decedent information needed by coroners, medical examiners, and funeral directors;
- Information necessary for cadaver, organ, eye, or tissue donation;
- Certain types of research (contact CMS for details);
- Necessity to disclose to avert serious health or safety threat; and
- Specialized government functions.

"Notice of Privacy Practices for Protected Health Information" (hereafter called "the Notice")

Physicians are required to give patients a written statement that describes the physician's privacy policies and his or her patients' privacy rights in plain language. Physicians are encouraged to obtain a written acknowledgment that patients received the statement, but if that is not possible, the physician should demonstrate that a good faith effort was made to attain a patient's signature. A chart note to that effect (or a standard printed statement describing the good faith effort in the chart) should suffice. The Notice must include its effective date of implementation and the name of a contact person in the practice who is available to answer patients' questions.

The Notice must be headed by the following statement:

"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

The Notice must tell patients that their PHI may be disclosed for the purposes of TPO, and it must include at least one example of each of these uses. *(Examples: Treatment—If your physician refers you to a specialist, s/he may fully disclose your PHI to that specialist to obtain his/her clinical opinion of your condition and/or care; Payment—Your physician will provide the minimum amount of information necessary to your health insurance company in order to obtain payment for the medical care you received; Operations—Your physician obtains services from his/her insurers or other business associates such as quality assessment, quality improvement, outcome evaluation, clinical guidelines development, and other similar services. Your doctor will share your PHI only to the extent necessary for receipt of those services. The recipients of your PHI are held to the same standard of confidentiality as your physician.)*

The Notice must inform patients of their individual health information privacy rights. They must be told that they have the right to:

- Request restrictions on disclosure of their PHI. They must also be told that their physician is not required to agree to their restriction request, but that if s/he agrees, the physician must make the amendment within 60 days.
- Receive confidential PHI communications via alternative means or locations (Example: They may ask that physicians send their bills to a post office box, rather than to their home mailing address; they may request faxed or emailed communication.);
- Inspect and obtain a paper copy of their PHI. They should be told that their request will be processed within 30 days (or less, if compelled to do so by state law), and that they may (or will) be charged a reasonable, cost-based fee for the copy;
- Request an amendment of their PHI. They must be told that their physician is not required to agree to such a request, particularly if the PHI was generated by someone else, or if the PHI is accurate and complete. The physician may require the request to be in writing, may require a reason for the request, and may inform others of the request for amendment. If a patient requests an amendment, and the physician denies his/her request, the patient may write an objection to the denial, and require that all related communication be documented and attached to future disclosures of the PHI;
- Receive a list of the disclosures – after the implementation of the Privacy Act – of their PHI for nonroutine, non-TPO uses, with the exception of those made in the interest of national security or a facility's directory (usually a hospital's list of admitted patients). The list must be compiled within 60 days of the request and must include the disclosure date, recipient's name, a description of the disclosed PHI, the purpose of the release or a copy of the authorization;
- Revoke previous authorizations for disclosure, except to the extent the information has already been disclosed as originally permitted;
- Obtain a copy of the Notice;
- File a formal complaint if their privacy rights were violated. The Notice must tell patients how to file a complaint and reassure them that no retaliatory action will be taken against them for doing so; and
- View the Notice on the practice website, if one exists.

The Notice must reflect state law when state law is contrary to and more stringent than HIPAA requirements. To learn what laws in your state must be included in the Notice, contact your local medical society.

The Privacy Policy, itself

The small office privacy policy, written for the physician(s) and staff, must describe in writing how

PHI will be created, distributed, retained, stored, retrieved, and destroyed. It must describe the plan by which patients are educated about the Privacy Act and how the Patients' Notice of Privacy will be distributed; the Policy must be congruent with the Notice. The Policy must include the agreement that the Business Associates (BA) will sign, and a copy of the authorization form patients must sign for release of PHI for nonroutine disclosures.

The Policy should be written in language that makes it meaningful, understandable, appropriate and relevant to the physicians and employees of the practice. Essentially, it must include descriptions or explanations of:

- The process by which patients may revoke their authorization for release of records;
- The uses and disclosures of TPO;
- The process by which patients' authorization is documented and retained;
- The special considerations related to psychotherapy notes, if applicable;
- The disclosures required by law, and others permitted without authorization;
- The persons (by individual or class of persons) who need access to PHI to carry out their duties;
- The conditions under which the practice will engage in marketing to patients, if at all;
- The conditions under which the practice will engage in fund raising, if at all;
- The confidential information to which patients have access;
- The process by which a patient can request information and the time frames for the physician's response (generally, within 30 days when information is on-site, unless state law is contrary and more stringent);
- The process by which a physician can deny access and how the patient may appeal the denial;
- The PHI that is maintained by specific BA, how the BA will modify the PHI (if at all), and how long it would take to retrieve the information from the BA, if needed;
- The reasonable cost-based fee the practice will charge patients for copying PHI;
- The reasons for which access to records would be denied and how the patient would be informed;
- The process by which a patient may request an amendment to his/her PHI, how quickly the physician must respond, how to proceed if the author of the information is no longer available, and how a request for an amendment will be accepted or denied;
- The process by which an accounting of nonroutine disclosures for up to a six-year period beginning no later than April 14, 2003, will be made available upon request;
- The agreements between the CE and the BA;
- The process by which patients may make complaints, how complaints will be documented, and how they will be resolved;
- The protections against retaliation for making a complaint;
- Appropriate administrative, technical, and physical safeguards implemented to ensure the privacy and confidentiality of PHI;
- A training plan to educate all employees about the Privacy Policy; and
- Sanctions against employees who violate the Privacy Policy.

Business Associate Agreement

Business Associates (BA) are persons or organizations who provide services to physicians that keep the machinery of a practice in motion, e.g., billing and collection services, claims processors, data analysis, quality assurance, accounting, accreditation, transcription, marketing consultant, financial services, administration, legal services, professional liability services, etc. In the context of HIPAA, BAs perform activities or functions that involve the use or disclosure of PHI. ("Conduits" of information, such as USPS, FedEx, UPS and other such entities are not considered BAs.) Business Associates must agree that they will not use or disclose PHI in any way contrary to the Privacy Act parameters with which the CE must comply. The signed BA agreement must include the BA's assurance that it will:

- Use and disclose PHI only as permitted under the contract and by law;
- Protect PHI to prevent unauthorized disclosure;
- Report any confidentiality violations to the CE or to the Department of Health and Human Services;
- Ensure that its agents abide by the same confidentiality restrictions;
- Make PHI available to patients when appropriately requested to do so;

- Make PHI available for amendment when appropriately requested to do so;
- Present an account of disclosures when appropriately requested to do so;
- Make available to the Secretary of Health and Human Services all information relating to privacy and disclosure if asked to do so; and,
- At the end of the contract with the CE, where it is possible and practicable, either return or destroy all PHI received from the CE in the course of business.

If a Business Associate breaches a patient's confidentiality, the CE is also in violation of the Privacy Act only if the CE was aware of the breach and took no action.

Violations and penalties

The Office of Civil Rights (OCR) is responsible for enforcement of HIPAA's Privacy Act. Generally speaking, it will investigate and prosecute penalties for noncompliance on the basis of complaints made to HHS. Civil penalties will be assessed at $100 per violation, and up to $25,000 per person per year. Persons who are criminally prosecuted under federal law for obtaining or disclosing PHI may be fined up to $50,000 and sentenced to one year in prison. If a person is convicted of obtaining or disclosing PHI under false pretenses, or for commercial or personal gain, or for malicious intent, that person may be fined up to $250,000 and sentenced for up to 10 years in prison.

Summary

HIPAA's Privacy Act is intended to increase medical professionals' protection of patients' confidential information in ways that are reasonable and appropriate, and to the scale of the size and nature of the practice. The Office of Civil Rights has said it will monitor compliance by investigating complaints, and will focus on facilitating compliance rather than administering sanctions.

Many physicians in solo or small group practices have always protected patients' PHI with care. Preparing the good faith documents that affirm their policies will probably be the most time-consuming aspect of compliance; once finished, their good practices will continue as they always have, well within the parameters of the Privacy Act.

Resources

Vendors, educators and organizations too numerous to adequately review and responsibly list for this newsletter offer products and services to aid physician compliance with HIPAA's Privacy Act. We encourage policyholders to exercise caution when considering purchase of HIPAA-related services or products. The following websites are known to have accurate Privacy Act information of interest to the small practice at no cost to the physician:

Office of Civil Rights
(This office enforces HIPAA's Privacy Act.)
www.hhs.gov/ocr/hipaa

Centers for Medicare and Medicaid Services (CMS)
www.cms.hhs.gov/hipaa

Workgroup for Electronic Data Interchange – Strategic National Implementation Process
www.wedi.org/SNIP

Phoenix Health Systems
www.hipaadvisory.com

American Medical Association
www.ama-assn.org

Please contact your local and state medical societies and associations for further information, additional resources, and preemptive analyses of state law.

Alaska State Medical Association
907/562-0304
Email: asma@alaska.net

California Medical Association
www.cmanet.org

Alameda-Contra Costa County Medical Association
510/654-5383
Email: accma@accma.org

San Francisco Medical Society
www.sfms.org

Hawaii Medical Association
www.hmaonline.net

Idaho Medical Association
www.idmed.org

How to reach MIEC:

Phone:

Oakland Office: 510/428-9411
Honolulu Office: 808/545-7231
Boise Office: 208/344-6378
Outside: 800/227-4527

Fax:

Loss Prevention: 510/420-7066
Oakland: 510/654-4634
Honolulu: 808/531-5224
Boise: 208/344-7903

Email:

Lossprevention@miec.com
Underwriting@miec.com
Claims@miec.com

MIEC on the Internet:
www.miec.com