

ED Legal Letter

The Essential Monthly Guide to Emergency Medicine Malpractice Prevention and Risk Management
From the publishers of *Emergency Medicine Reports* and *ED Management*

Register now for audio conference
on new HIPAA privacy rule! (See p. 132-1)

American Health Consultants Home Page—<http://www.ahcpub.com> For more information, call (800) 688-2421.

CME for Physicians—<http://www.cmeweb.com>

EXECUTIVE EDITOR

James Hubler, MD, JD, FCLM, FACEP, FAAEM

Clinical Instructor of Surgery, Department of Emergency Medicine, University of Illinois College of Medicine at Peoria; EMS Medical Director, Central Illinois Center for Emergency Medicine, OSF Saint Francis Hospital, Peoria, IL

EDITORIAL BOARD

Kay Ball, RN, MSA, CNOR, FAAN

Perioperative Consultant/Educator, K&D Medical, Lewis Center, OH

Robert Bitterman, MD, JD, FACEP

Director of Risk Management and Managed Care, Department of Emergency Medicine, Carolinas Medical Center, Charlotte, NC

Paul Blaylock, MD, JD, FACEP

Emergency Medicine Physician, Southwest Washington Medical Center, Emanuel Medical Center; Member, Board of Governors, American College of Legal Medicine; Retired of Counsel, Miller, Nash, Wiener, Hager & Carlsen, Attorneys at Law, Portland, OR

Theresa Rodier Finerty, RN, MS

Director, Emergency and Trauma Services, OSF Saint Francis Medical Center Peoria, IL

Michael A. Gibbs, MD, FACEP

Chief, Department of Emergency Medicine, Maine Medical Center, Portland, ME

Jonathan D. Lawrence, MD, JD, FACEP

Emergency Physician, St. Mary Medical Center, Medical-Legal Consultant, Long Beach, CA

J. Tucker Montgomery, MD, JD, FCLM

Montgomery & Pierce, Knoxville, TN

Gregory P. Moore, MD, JD

Department of Emergency Medicine, Indiana University School of Medicine, Indianapolis

Jane A. Severson, RN, MS, MHSA,

University of Michigan Health System, Ann Arbor, MI

Daniel J. Sullivan, MD, JD, FACEP

Chairman, Department of Emergency Medicine, Ingalls Memorial Hospital; Associate Professor of Emergency Medicine, Rush Medical College, Harvey, IL

William Sullivan, DO, JD, FCLM

Clinical Instructor, Department of Emergency Medicine, Midwestern University, Downers Grove, IL; Clinical Assistant Professor, Department of Emergency Medicine, University of Illinois, Chicago

Jay C. Weaver, JD, EMT-P

Boston Public Health Commission Emergency Medical Services; Adjunct Faculty, Northeastern University, Boston

James G. Zimmerly, MD, JD, MPH, FACPM,

FCLM, Past President, American College of Legal Medicine, Adjunct Professor of Law, Georgetown University Law Center; Associate Professor of Preventive Medicine, University of Maryland School of Medicine, Baltimore

New HIPAA privacy mandates create ED compliance concerns

By **Jay C. Weaver, JD, EMT-P**, Boston Public Health Commission Emergency Medical Services; Adjunct Faculty, Northeastern University, Boston, MA.

Editor's Note: *A patient's right to privacy has risen to an unprecedented level in the United States this year with the development of strict regulations under the Health Insurance Portability and Accountability Act (HIPAA). While increasing patient access, the HIPAA regulations also limited disclosure. The new regulations will protect patient rights while simultaneously creating an enormous burden for emergency departments (EDs). There is no doubt that this new federal mandate will create compliance problems and uncertainty that will rival those of the Emergency Medical Treatment and Labor Act (EMTALA) regulations. Violations of HIPAA rules may subject providers to civil suits, monetary penalties, and criminal sanctions that include potential imprisonment. This issue of ED Legal Letter details how these changes will affect ED operations and outlines strategies for compliance.*

Introduction

On April 14, 2002, the U.S. Department of Health and Human Services (HHS) issued a regulation that will change forever the operation of EDs.¹

HHS's Standards for Privacy of Individually Identifiable Health Information—more commonly known as the "Privacy Rule"—preempts dozens of conflicting state confidentiality laws, establishing in their place a single, comprehensive, national health information privacy requirement.² Authorized by Congress under HIPAA, this regulation guarantees increased access to medical records by patients, while at the same time limiting the disclosure of personal health information to others.³ With few exceptions, the Privacy Rule will govern every health care provider in the United States.^{4,5} The new regulation, therefore, will dictate the record-keeping practices of virtually every ED in the nation.

Not everyone supports the Privacy Rule in its current form. Privacy advocates have complained that, even after several revisions, the final version contains too many loopholes, particularly with regard to marketing uses and the access of medical records by law enforcement officials.^{6,7} Others feel that the

new regulation will hinder public health, safety, and welfare initiatives.⁸ The anticipated cost of implementing the Privacy Rule has sparked debate, as well.⁹

The Bush Administration has implemented the Privacy Rule in spite of these controversies.¹⁰ Health care providers, including EDs, must comply with the new standards by April 14, 2003.¹¹ This article will describe the purpose and historical development of the Privacy Rule, the ways in which this new regulation will affect ED operations, and strategies for coping with the changes to come.

Purpose and Development of the Privacy Rule

The transition from paper to electronic record keeping has benefited the health care industry and patients alike. Clinicians share information with consultants and laboratories immediately, thereby permitting more rapid diagnosis and more effective treat-

ment. Billions of dollars of annual insurance claims are processed more efficiently. Electronic data collection has enhanced scientific research and allows for the earlier detection of communicable disease outbreaks by public health officials.

These advances have come at a cost to personal privacy, however. America's health care system no longer consists exclusively of one-on-one relationships between physicians and patients. Rather, it includes "managed care providers" and complex "health care delivery networks." As a result, many more people have the ability to view personal health information than ever before. During a typical hospital stay, an average of 150 employees—from billing clerks to surgeons—have access to a patient's medical records.¹² This problem is compounded by the fact that hospitals routinely share patient information with outside entities, including insurance companies, pharmacies, benefits managers, and accrediting organizations. Often these disclosures take place without the knowledge of the patient.¹³

Concerns about patient privacy are not merely theoretical. They are grounded in reality. As the following cases illustrate, the use of electronic medical records can contribute to devastating breaches of personal privacy.

- While working the bugs out of its new patient scheduling system, the University of Michigan health system accidentally posted thousands of patient records on the Internet. The information remained accessible to the public until a medical student discovered the error two weeks later.¹⁴
- An employee of the Tampa, FL, health department left work with a computer disc containing the names of 4000 HIV-infected patients and mailed it to a pair of newspapers.¹⁵
- A convicted child rapist obtained a job at a Massachusetts hospital. Using the password of a former employee, he gained access to nearly 1000 electronic medical records, which he used to place obscene phone calls to young girls.¹⁶
- While computerizing its medical records in 1995, a New England health maintenance organization, Harvard Community Health Plan, inadvertently gave many of its employees access to the psychotherapy notes of its patients.¹⁷
- After purchasing a used computer in 1997, a Nevada woman discovered that its memory contained the prescription records of the pharmacy that had owned it previously. These records included

ED Legal Letter[™], ISSN 1087-7341, is published monthly by American Health Consultants, 3525 Piedmont Road N.E., Bldg. 6, Suite 400, Atlanta, GA 30305.

Vice President/Publisher: Brenda Mooney
Editorial Group Head: Valerie Loner
Managing Editor: Allison Mechem
Production Editor: Nancy McCreary
GST Registration Number: R128870672.
Periodicals postage paid at Atlanta GA 30304.
POSTMASTER: Send address changes to *ED Legal Letter*, P.O. Box 740059, Atlanta, GA 30374.

Copyright 2002 by American Health Consultants. All rights reserved. No part of this newsletter may be reproduced in any form or incorporated into any information-retrieval system without the written permission of the copyright owner.

Back issues: \$77. Missing issues will be fulfilled by customer service free of charge when contact ed within one month of the missing issue's date.

Opinions expressed are not necessarily those of this publication, the executive editor, or the editorial board. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought in specific situations.



Now available on-line at www.ahcpub.com/online.html

Statement of Financial Disclosure

To reveal any potential bias in this publication, and in accordance with Accreditation Council for Continuing Medical Education guidelines, Dr. Hubler (executive editor); Advisory Board members Ball, Bitterman, Blaylock, Finerty, Gibbs, Lawrence, Montgomery, Moore, Severson, Dan Sullivan, William Sullivan, and Weaver have reported no relationships with companies having ties to the field of study covered by this CME program.

Subscriber Information

Customer Service: (800) 688-2421

Customer Service E-Mail Address:
customerservice@ahcpub.com
Editorial E-Mail Address: allison.mechem@ahcpub.com
World Wide Web: <http://www.ahcpub.com>

Subscription Prices

United States: \$459 per year
Multiple Copies:
2-9 additional copies: \$367 each.
10+ copies: \$275 each.
Canada: \$489 per year plus GST
Elsewhere: \$489 per year

Accreditation

American Health Consultants is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide CME for physicians. American Health Consultants designates this CME activity for 12 credit hours of Category 1 of the Physician's Recognition Award of the AMA. *ED Legal Letter*[™] is also approved by the American College of Emergency Physicians for 12 hours of ACEP Category 1 credit. This CME activity was planned and produced in accordance with the ACCME Essentials.

This continuing education program is sponsored by American Health Consultants, which is accredited as a provider of continuing education in nursing by the American Nurses Credentialing Center's Commission on Accreditation. Provider approved by the California Board of Registered Nursing for approximately 12 contact hours. Provider #CEPT10864.

Questions & Comments

Please contact Allison Mechem,
Managing Editor, at
allison.mechem@ahcpub.com
or (404) 262-5589.

patient names, addresses, social security numbers, and lists of all medicines purchased by the pharmacy's customers.¹⁸

Confidentiality long has been recognized as a prerequisite to effective treatment.¹⁹ Patients who lose confidence in the discretion of their clinicians are more likely to withhold information crucial to diagnosis and treatment, and even to provide misleading information.²⁰ In the most extreme cases, patients "doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by insurance, and avoid care altogether."²¹

Until recently, laws protecting confidentiality were enacted almost exclusively by the states.²² In some instances, federal regulations have required hospitals to ensure the confidentiality of patient records.²³ These provisions apply only to facilities participating in the Medicare program, and their language could be construed as applying only to certain forms of records.²⁴ Other federal statutes, such as the Privacy Act of 1974 and the Americans with Disabilities Act, create limited individual health privacy rights, but almost never apply to care provided in EDs.^{25,26}

Gaps in protection prompted Congress to establish universal privacy protections as part of its Health Insurance Portability and Accountability Act of 1996.²⁷ A remnant of the 1993 Clinton health reform plan, HIPAA amended the Employee Retirement Security Act (ERISA), the Public Health Services Act, and the Internal Revenue Code with the goals of facilitating health insurance availability and continuity, combating health care fraud and abuse, and establishing more favorable tax treatment for various health-related benefit plans.²⁸ The Administrative Simplification subtitle of HIPAA provided that if Congress did not enact health privacy standards within three years, this responsibility would shift to the Secretary of Health and Human Services.²⁹ Congress defaulted on its self-imposed deadline, and on Nov. 3, 1999, HHS Secretary Donna Shalala published a set of proposed rules establishing standards for the protection of individually identifiable health information.^{30,31}

What followed can be described only as chaos. Within a year, HHS received more than 52,000 public comments about the proposed regulations.³² Secretary Shalala issued a revised Privacy Rule in December 2000, but the resulting 400-page document probably created more confusion than it resolved.³³ HHS received another deluge of telephone calls, e-mails, letters, and other forms of inquiry that reflected "sub-

stantial misunderstanding" about the new regulations, as well as "great concern over the complexity of the Privacy Rule."³⁴

Recognizing that the new regulations would have "unintended effects" on health care if implemented as proposed, Shalala's successor, Tommy G. Thompson, ordered further modification of the Privacy Rule in March 2002.^{35,36} This time, the public responded with more than 11,000 comments in just 30 days.³⁷ Undeterred by the controversial nature of the proposed regulations, the Secretary published final modifications to the Privacy Rule on August 14, 2002.³⁸ Health care providers were given one year from that date to comply with the new standards.³⁹

Privacy Rule Implications for the ED

To comply with HHS's new privacy regulations, ED practitioners and administrators must first understand them. This section will outline the Privacy Rule provisions most relevant to ED practice.

Individuals and Entities Covered by the Privacy Rule. The Privacy Rule applies to health plans, health care clearinghouses, and health care providers.⁴⁰ "Health care provider," in turn, has been defined by HHS for HIPAA purposes as "a provider of health services [as defined under the Social Security Act] and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."⁴¹ The Privacy Rule, therefore, regulates the conduct of physicians and hospitals, as well as ancillary ED personnel such as nurses, social workers, and emergency medical technicians.⁴²

Not all health care providers are subject to the Privacy Rule, however. Because Congress intended HIPAA to promote the electronic exchange of health information, the Privacy Rule applies only to health care providers who utilize electronic information technology.^{43,44} Health care providers who store or transmit medical records electronically must adhere to the Privacy Rule's requirements at all times, even when storing or transmitting medical records in some other form.⁴⁵ Those who record all of their patient information in paper charts, on the other hand, are excluded from the Rule's coverage.⁴⁶ Thus, a physician in private practice who maintains only paper records *and who never stores or transmits those records electronically* is free to ignore the Privacy Rule, while clinicians at an ED with a state-of-the-art record-keeping system must adhere to HHS standards even when casually dis-

cussing a patient's condition with colleagues.

Information Covered by the Privacy Rule. HHS originally intended the Privacy Rule to apply only to health information stored or transmitted electronically.⁴⁷ Health information that had existed solely on paper, therefore, would have been excluded from coverage.⁴⁸

Privacy advocates convinced HHS during the public comment period to expand the scope of covered information.⁴⁹ As a result, the Privacy Rule now applies to "all individually identifiable health information in any form, electronic or non-electronic, that is held or transmitted by [an entity that utilizes electronic information technology]. This includes individually identifiable health information in paper records that never has been electronically stored or transmitted."⁵⁰ HHS refers to the information covered by the Privacy Rule as "protected health information."⁵¹

Despite this seemingly broad scope of coverage, some health information remains exempt from the Privacy Rule's standards. By answering the questions in Table 1, ED administrators and practitioners can determine whether a patient's health information is "protected" under HHS's new regulations.

The Privacy Rule permits health care providers to "de-identify" protected health information, thereby eliminating restrictions on its use for research or other purposes.⁵² This may be accomplished in two ways. First, the health care provider may document the findings of an expert who, having applied "generally acceptable statistical and scientific principles and methods," determines that there is a "very small risk" that the information in question can be used by others to identify a subject of that information.⁵³

Alternatively, the health care provider may utilize the Privacy Rule's "safe harbor" method, which deems protected health information to be de-identified as soon as 18 enumerated elements have been removed.⁵⁴ While still complicated, the latter option undoubtedly will prove less burdensome than the utilization of an expert. Table 2 describes the safe harbor de-identification process.

Health care providers may assign a code to de-identified information that will permit subsequent re-identification, as long as the health care provider does not disclose the code to outside entities, and as long as others cannot decipher the code.⁵⁵

Restrictions on Use and Disclosure of Protected Health Information. The Privacy Rule imposes a broad duty of confidentiality on health care providers.

Table 1. Protected Health Information

1. Does the ED or its parent hospital ever store or transmit patient health information electronically?¹⁵⁴
2. Does the information pertain in any way to an individual's medical condition, health care, or payment for the provision of health care?¹⁵⁵
3. Is there a reasonable basis to believe that the information will permit identification of an individual?¹⁵⁶
4. Does the information consist of material other than records covered by the Family Educational Right and Privacy Act?¹⁵⁷

If the answer to all of these questions is "yes," the information qualifies as "protected" and the ED must handle it in accordance with the Privacy Rule. If the answer to any question is "no," the information falls outside the scope of the rule and is subject only to applicable state privacy laws.

Physicians, nurses, and other practitioners are permitted to disclose protected health information only under defined circumstances.⁵⁶ Confidentiality, therefore, has become the rule under federal law, rather than the exception.

The new regulations do not guarantee confidentiality at all times, however. Health care providers remain free to use and disclose protected health information for purposes of treatment, payment, and health care operations.⁵⁷ "Health care operations" include not only the actual provision of care, but also the administrative, financial, and legal activities necessary to support that care.⁵⁸ For ED personnel, this means quality assessment and improvement activities, the development of clinical protocols, complying with accreditation and licensing requirements, and the like.⁵⁹

HHS has embedded within its regulations at least two dozen such exceptions to the general ban on health information disclosure. The most obvious of these exceptions pertains to the relationship between clinician and patient. Section 164.502 of the Privacy Rule expressly permits the disclosure of protected health information to the individual who is the subject of that information.⁶⁰ (A version of the Privacy Rule proposed under the Clinton Administration would have required health care providers to obtain written consent from their patients before using or disclosing protected health information.⁶¹) Without this common-sense provision, the Privacy Rule would produce the illogical result of prohibiting clinicians from discussing test results and diagnoses with the very patients upon whom those tests had been performed.

Effective April 14, 2003, direct treatment

providers, including ED personnel, must provide each patient with a written “privacy practices notice” that describes, among other things, the potential uses and disclosures of protected health information.^{62,63} The patient must receive this information on the first day of treatment, or, in an emergency, “as soon as reasonably practicable” afterward.^{64,65} See Table 3 for a description of the required elements.

While health care providers are not required to seek consent under the Privacy Rule, they may do so in addition to providing the required notification.⁶⁶ This will be the prudent course of action in the vast majority of patient encounters. The Privacy Rule grants health care providers complete discretion when adopting these optional consent policies.⁶⁷

Under the final version of the Privacy Rule, direct care providers must make a good faith effort to obtain from each patient a written acknowledgment that he or she has received the provider’s privacy practices notice.⁶⁸ HHS feels that this process, like a request for consent, will prompt individuals to discuss privacy-related concerns with their health care providers before the onset of care.⁶⁹ ED personnel should note that the Privacy Rule does not require direct care providers to seek acknowledgment during “emergency treatment situations.”⁷⁰

The Privacy Rule does not mandate a particular form of written acknowledgment.⁷¹ The preamble to the final version of the rule suggests that direct care providers can satisfy this requirement by having patients initial a copy of the notice, sign a list, or, when the notice has been delivered electronically, by capturing an electronic response.⁷² Providers who fail to obtain such an acknowledgment must document their efforts, however, along with the reasons why the acknowledgment could not be obtained.⁷³

The December 2000 version of the Privacy Rule did not address incidental uses and disclosures of protected health information.⁷⁴ Health care providers subsequently expressed concern that the inflexibility of the Privacy Rule would substantially interfere with the timely provision of health care.⁷⁵ Accordingly, HHS has added a provision that allows health care providers to use and disclose information in ways not expressly permitted by the rule, but which are necessary to routine health care practices.⁷⁶ Without this provision, ED practitioners might be prohibited from utilizing sign-in sheets at triage, maintaining bedside charts, or calling out patients’ names in a waiting room, because each of these acts might constitute a

Table 2. “Safe Harbor” De-Identification of Protected Health Information

Protected health information becomes “de-identified,” thereby falling outside the scope of Privacy Rule protection, once the following elements have been removed with regard to the patient, the patient’s relatives, the patient’s household members, and the patient’s employers:¹⁵⁸

1. Names
2. Geographic information smaller than a state, including street addresses, cities, counties, and at least the final two digits of ZIP codes
3. Elements of dates directly related to the patient, including dates of birth, admission, discharge, and death. Years, such as the age of the patient, may be retained, except when the year pertains to a patient older than 90 years.
4. Telephone and fax numbers
5. E-mail addresses, Web universal resource locators (URLs), and Internet protocol address numbers
6. Social security, medical record, health plan beneficiary, certificate, license, and account numbers
7. Vehicle identifiers and serial numbers, including license plate numbers
8. Device identifiers and serial numbers
9. Biometric identifiers, including finger and voice prints
10. Full-face photographs and comparable images

HHS does not consider protected health information to be de-identified when the health care provider has actual knowledge that the remaining information could be used to identify a subject of the protected information.¹⁵⁹ Where a physician has treated a celebrity, for example, he may not disclose protected information about the patient—even after he has deleted the 18 enumerated “safe harbor” elements—if he knows that the circumstances surrounding the patient’s hospitalization will enable the public to deduce the patient’s identity.

prohibited disclosure of protected information.⁷⁷ The final version of the Privacy Rule allows these “incidental” activities, however.

Uses and Disclosures of Protected Information for Non-Routine Purposes. Health care providers who wish to use or disclose protected health information for purposes other than treatment, payment, and health care operations must obtain prior authorization from the patient.⁷⁸ To be valid, the authorization must be written in plain language, and must contain several “core elements” and notification statements.⁷⁹⁻⁸¹ An authorization is considered defective, and therefore invalid, once it has been revoked by the patient, or has expired.^{82,83} Authorizations containing false material information and those that have not been filled out

Table 3. Notice of Privacy Practices: Required Elements

Direct treatment providers, including EDs, soon will be required to provide each patient with detailed information about their privacy practices. The notification must be written in plain language, and must contain the following elements:¹⁶⁰

1. The prominently displayed phrase, *"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."*
2. A description and at least one example of how the health care provider can use and disclose protected health information for the purposes of treatment, payment, and health care operations, and a description of how the health care provider can use and disclose protected health information without the patient's consent or authorization. These descriptions must reflect any applicable laws more stringent than the Privacy Rule.
3. A statement that the health care provider will make other uses and disclosures only with the patient's written authorization, and that the patient has the right to revoke authorization previously granted.
4. A statement advising the patient of the following rights:
 - The right to request a restriction on uses and disclosures, including a statement that the health care provider need not comply with such requests.
 - The right to receive confidential communications of protected health information, as well as the right to request and receive these communication via a specified mode.
 - The right to inspect and copy certain protected health information.

- The right to amend protected health information.
 - The right to receive an accounting of certain disclosures.
 - The right to obtain a paper copy of the health care provider's privacy practices notice upon request.
5. A statement that the health care provider is required by law to maintain the privacy of protected health information; that the health care provider must abide by the terms of its privacy practices notice, and, if the health care provider intends to modify its privacy practices, a statement that this right has been reserved.
 6. A statement advising patients of the method by which they may complain about privacy violations to the health care provider and to the Secretary of HHS, and that privacy complaints will not cause retaliation.
 7. The identity and telephone number of an individual or office that can provide additional information about the health care provider's privacy practices.
 8. The effective date of the notice.

Health care providers who intend to contact patients with appointment reminders, information about available health-related services, or fund-raising requests must include separate statements to this effect in their notices.¹⁶¹ Privacy practices notices may be delivered via e-mail, but the patient retains the right to receive a paper version of the notice upon request or when the health care provider knows that electronic delivery has failed.¹⁶² Health care providers who post information about their services on a web site must display a privacy practices notice along with that information.¹⁶³

completely with respect to core elements also are defective.^{84,85} Table 4 describes the essential components of a valid authorization.

Health care providers generally may not require a patient to grant use and disclosure authorization as a precondition to receiving care.⁸⁶ In fact, a patient's refusal to sign an authorization justifies the withholding of treatment only in two circumstances: 1) when the treatment is research-related; and 2) when care is rendered solely for the purpose of disclosure to a third party.^{87,88} Thus, an ED physician may refuse to allow a patient to participate in a research study until the patient completes an authorization. Similarly, the physician may decline to grant medical clearance for admission to an independent substance-abuse program in the absence of such an authorization.

Authorizations may not be combined with any other document to create a compound authorization, except when the authorization pertains to research studies or psychotherapy notes.⁸⁹ These authorizations may be combined with authorizations of the same kind.⁹⁰ Authorizations also may be combined

when they serve as a permissible precondition to treatment.⁹¹

Patients may revoke authorizations at any time, as long as they do so in writing.⁹² Health care providers who seek authorizations must provide a signed copy of the authorization to the patient, whether the patient requests a copy or not.⁹³

Amount of Information to be Used or Disclosed. When using or disclosing protected health information, health care providers must make "reasonable efforts" to use or disclose the minimum information necessary to accomplish the intended purpose of the use, disclosure, or request.⁹⁴ This "minimum necessary" standard does not apply, however, when the use or disclosure is made to another health care provider for treatment purposes, or when it is made to the individual who is the subject of that information.⁹⁵ This standard also does not apply to uses and disclosures authorized by the patient in accordance with Privacy Rule standards, or when the use or disclosure is required by law, as in the case of disclosures made for workers' compensation purposes.^{96,97}

Table 4: Authorization for Non-Routine Uses and Disclosure: Core Elements and Required Statements

TO BE VALID, AN AUTHORIZATION MUST BE WRITTEN IN PLAIN LANGUAGE AND CONTAIN AT LEAST THE FOLLOWING "CORE ELEMENTS":¹⁶⁴

1. A "meaningful and specific" description of the information to be used or disclosed
2. Identity of the persons or class of persons authorized to make the use or disclosure
3. Identity of the authorized recipients of the information
4. Purpose of the use or disclosure. "At the request of the individual" is sufficient when the patient initiates the authorization and does not provide a statement of purpose.
5. Expiration date or event. "End of the research study" or "None" is sufficient.
6. Signature of the individual or the individual's authorized personal representative and the date. If the authorization is signed by a personal representative, a description of the representative's authority to act for the individual also must be included.

THE FOLLOWING STATEMENTS ALSO MUST APPEAR ON THE AUTHORIZATION DOCUMENT:¹⁶⁵

1. A statement that the individual has the right to revoke the authorization and either a description of the exceptions to this right and methods of exercising it, or a reference to the applicable privacy practices notice.
2. A statement describing the extent to which the health care provider may condition treatment, enrollment, or benefits eligibility on the authorization.
3. A statement that information disclosed pursuant to the authorization might be redisclosed by the recipient, and that such information would no longer be subject to Privacy Rule protection.

The Privacy Rule does not prescribe a particular form of wording for these statements. Rather, the statement is sufficient as long as it "places the individual on notice" regarding the privacy rights to which the statement refers. Health care providers may include other information in their authorization forms, as long as that information does not conflict with the core elements and required statements.¹⁶⁶

Uses of Protected Health Information. The Privacy Rule requires health care providers to obtain the patient's written authorization before using protected health information for marketing purposes, except when the communication is limited to a face-to-face encounter or the exchange of a promotional gift of nominal value.⁹⁸ Marketing is defined by HHS as "communication about a product or service that encourages recipients of the communication to purchase or use the product or service."⁹⁹ Excluded from the definition of marketing, however, are communications pertaining to the treatment, case management, or care coordination of the patient; discussions about alternative treatments, health care providers, or care settings; and a description of health-related products and services provided through a benefit plan.¹⁰⁰ This represents a significant departure from the "opt-out" approach proposed under the original version of the Privacy Rule.¹⁰¹

Health care providers are permitted to disclose protected health information to business associates, as long as the health care provider has obtained a "satisfactory assurance" in writing that the business associate will appropriately safeguard the information.¹⁰² "Business associates" include those who provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, financial,

data analysis, utilization review, quality assurance, or billing services for the health care provider, but are not members of the health care provider's workforce.¹⁰³ Thus, an ED clerk may forward medical records to a billing company, without authorization from the facility's patients, once the billing company has provided the hospital with a written assurance that it will use and disclose that information only as permitted by the Privacy Rule and state law.

The final version of the Privacy Rule permits disclosure of protected health care information to government bodies under defined circumstances. Health care providers may disclose protected health information to law enforcement officials who need that information to "identify or apprehend an individual" in the presence of a "serious and imminent threat" to health or safety, or where the patient is thought to be a victim of abuse, neglect, or domestic violence.^{104,105} Limited information may be disclosed to law enforcement officials for the purposes of identifying or locating suspects, witnesses, and missing persons.¹⁰⁶ Privacy advocates have objected strenuously to these provisions, alleging that the rule provides law enforcement officials with "unchecked access to individual medical records, without a warrant or even notice to the individual whose medical records are at issue."¹⁰⁷

Protected information also may be disclosed to

public health authorities for use in disease prevention and control, and to the Food and Drug Administration (FDA), to enable investigations and recalls of potentially defective products.¹⁰⁸ Where a public health authority has the legal authority to notify individuals at risk of contracting or spreading communicable diseases, the Privacy Rule allows disclosure of protected health information to those individuals.¹⁰⁹

(For discussion of strategies for coping with the Privacy Rule, see Insert.)

Patient Access

The Privacy Rule does more than just restrict uses and disclosures of health information. It also standardizes the right of access to health information by patients.

Under the Privacy Rule, individuals enjoy the right to inspect their medical records upon request.¹¹⁰ They also have the right to obtain copies of those records. Health care providers must act on a patient's request for access within 30 days, except when the requested information is not maintained or accessible on-site.¹¹¹ In those instances, the health care provider must act within 60 days.¹¹²

This right of access is not absolute, however. ED personnel need not disclose psychotherapy notes, nor must they disclose to patients information that the health care provider reasonably believes will be used in any kind of legal proceeding.¹¹³ Requests for information that falls within the scope of the Clinical Laboratory Improvements Amendments of 1988 also may be denied by the health care provider.¹¹⁴

HHS has endeavored to remain neutral regarding the right of parents to access the health records of their minor children.¹¹⁵ This approach recognizes three competing interests: 1) the continued interest of the minor, already recognized in every state, to seek limited forms of health care without parental consent, such as HIV testing; 2) the interest of the parent in making health care decisions about their children; and 3) the interest of state medical boards in establishing ethical codes without federal interference. To reconcile these interests, HHS has deferred to the states on the issue of parental access to medical records, permitting health care providers to disclose protected health information to parents in a manner consistent with applicable state law.¹¹⁶ However, the rule does permit disclosures to parents that are necessary to avert a "serious and imminent threat

to the health or safety of the minor."¹¹⁷

Patients have a right to receive an accounting of disclosures made by their health care providers, except where the disclosure pertains to treatment, payment, or health care operations, or where the disclosure occurred for law enforcement purposes.^{118,119} The accounting must include disclosures made within six years prior to the request.¹²⁰ It must specify the date of the disclosure; the identities of the people who received the disclosure and their addresses, if known; and a brief description of the basis for the disclosure or a copy of the patient's written authorization or request for disclosure.¹²¹⁻¹²³ The most recent version of the Privacy Rule streamlines the accounting process with regard to disclosures pertaining to public health activities and research.^{124,125}

Patients who believe that their medical records contain errors can require their health care providers to amend that information within 60 days, unless the health care provider maintaining those records replies in writing that the records are "accurate and complete," or that someone else created the records in question.¹²⁶ Health care providers and patients who continue to disagree about the accuracy of the record have the right to add to that record a statement or rebuttal, as appropriate.¹²⁷

Documentation

The Privacy Rule requires health care providers to document many of their decisions and activities. A hospital, for example, must document all of the complaints it receives pertaining to Privacy Rule violations, as well the disposition of those complaints.¹²⁸ Hospitals also must document all communications that the Privacy Rule requires to be in writing, details of compliance training the hospital provides to its employees, and appointments of privacy officials and a contact person.¹²⁹ Signed use and disclosure authorizations must be documented as well.

Hospitals must adopt Privacy Rule policies and procedures prior to the April 14, 2003, compliance date.¹³⁰ These policies must be amended periodically to reflect changes in the law.¹³¹ Health care providers, including hospitals, must apply appropriate sanctions against employees who violate the Privacy Rule, and must document those sanctions.¹³²

Hospitals must retain documentation required by the Privacy Rule for six months from the date of its creation or the date it was last effective, whichever

is later.¹³³ In addition, the Privacy Rule requires health care providers to retain all records deemed necessary by the HHS Secretary to a determination of compliance.¹³⁴

Penalties

Violation of the Privacy Rule can result in tort liability, and in civil and criminal sanctions. While a first offense for a general violation carries a fine of just \$100, anyone who knowingly obtains or discloses individually identifiable health information in violation of the rule can be fined up to \$50,000, imprisoned for as much as a year, or both.^{135,136} When the violation occurs under false pretenses, the maximum penalty increases to \$100,000 and five years' imprisonment. Those who violate the rule for "commercial gain" or "malicious harm" face the stiffest penalties—a \$250,000 fine, 10 years in prison, or both.

Enforcement. Privacy advocates have accused HHS of creating a regulation without teeth.¹³⁷ Indeed, this may constitute a valid complaint. The Privacy Rule establishes an enforcement procedure under which patients may file complaints with the health care provider and Secretary of HHS.¹³⁸ The rule does not require the Secretary to act on those complaints, however, or even to investigate them.¹³⁹ Rather, the Privacy Rule's Compliance and Enforcement Subpart specifies that the Secretary "may" investigate patient complaints. Health care providers must furnish protected health information to HHS for this purpose upon request of the department.¹⁴⁰

The Privacy Rule also does not establish a private right of action.¹⁴¹ In other words, patients cannot sue their health care providers for violating the Privacy Rule.¹⁴² This does not mean that ED personnel can afford to become lax when handling protected health information, however. The Privacy Rule does not preclude tort actions under state law for privacy invasion, and health care providers can face substantial fines or even jail time if an investigation by the Secretary does reveal evidence of a Privacy Rule violation.¹⁴³

Conflicts of Law

HHS has designed the Privacy Rule to enhance state privacy laws, not simply to replace them.¹⁴⁴ To accomplish this goal, the Privacy Rule preempts contrary provisions of state law, except where those provisions are more stringent.¹⁴⁵ The Privacy Rule there-

fore establishes a floor of protections, applicable to all Americans, that is supplemented by the laws of some states.¹⁴⁶

Twenty states impose statutory disclosure restrictions that extend beyond the scope of the Privacy Rule.¹⁴⁷ Two of these states, Wisconsin and Rhode Island, have enacted comprehensive privacy legislation that applies to virtually all health care providers within their jurisdictions.¹⁴⁸ Rhode Island's Confidentiality of Health Care Communications and Information Act, for example, imposes disclosure restrictions on anyone in that state who possesses a patient's confidential health information.¹⁴⁹ Thus, it remains possible for an ED practitioner to be penalized for failing to obtain consent, even though HHS has deleted the consent requirement from the Privacy Rule.

When faced with a conflict between state law and the Privacy Rule, ED personnel must distinguish between mandatory and permissible disclosures. The Privacy Rule permits health care providers to make disclosures mandated by state law, including reports of birth, death, child abuse, and disease or illness.^{150,151} ED practitioners comply with both state and federal law when they make disclosures that are required by state law. Where state law only permits a particular type of disclosure, however, the practitioner should refrain from making the disclosure, because to do so would violate the Privacy Rule.¹⁵² This principle applies as well to conflicts between the Privacy Rule and other federal laws.¹⁵³

Endnotes

1. See U.S. Dept. of Health & Human Servs., *HHS Issues First Major Protections for Patient Privacy*, HHS News, Aug. 9, 2002, at 1.
2. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,801 (2000). See Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,182 (2002).
3. Administrative Simplification Act, Pub. L. No. 104-191, 110 Stat. 2033 (1996).
4. See, e.g., Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.500 (2002). See also 65 Fed. Reg. at 82,488 (clarifying that the Privacy Rules does not apply to federal agencies when providing health care to foreign citizens in other countries).
5. 45 C.F.R. § 164.500.
6. Amy Goldstein, *HHS Issues Privacy Rules for Use of Health Records*, Washington Post, Aug. 10, 2002, at A1. See 67 Fed. Reg. 53,185-90 (2002).
7. See Health Privacy Project, *Summary of New Federal Health Privacy Regulations*, (visited Sept. 3, 2002) <<http://healthprivacy.org>>; American Civil Liberties Union, *ACLU Dismayed at Implementation of Flawed Medical Privacy Regulations* (August 9, 2002) (press release); Institute for Health Freedom, *Update on the Federal Medical Privacy Rule: Questions and Answers*, (last modified Apr. 1, 2002) <<http://forhealthfreedom.org>>.
8. See Goldstein, *supra* note 6, at A1; 65 Fed. Reg. at 82,471-72; 67 Fed. Reg. at 53,198-217.

9. See Institute for Health Freedom, *President Bush Orders Final Medical Privacy Rule to Take Effect*, (April 12, 2001) (press release).
10. See U.S. Dept. of Health & Human Servs., *supra* note 1; Goldstein, *supra* note 6, at A1.
11. 42 U.S.C. § 1360d-4 (2002); 45 C.F.R. § 164.534.
12. See 65 Fed. Reg. at 82,466.
13. See *id.*
14. See Jodi Upton, *U-M Records End Up on Web*, Detroit News, Feb. 12, 1999, at A1.
15. See David L. Coleman, *Who's Guarding Medical Privacy?*, Business & Health, Mar. 1999, at 30.
16. See John Riley, *Case Study: With Old Password, Cracking the Code*, Newsday, Mar. 31, 1996, at A30.
17. See Alison Bass, *HMO Puts Confidential Records Online*, Boston Globe, Mar. 7, 1995, at A1.
18. New York Times, April 4, 1997; New York Times, April 12, 1997.
19. See Massachusetts Medical Society, Patient Privacy and Confidentiality 14 (1996).
20. See Health Privacy Working Group, Best Principles for Health Privacy 9 (1999); 65 Fed. Reg. at 82,468.
21. See *id.*
22. See 65 Fed. Reg. at 82,463; Health Privacy Project, *The State of Health Privacy: An Uneven Terrain*, <http://www.georgetown.edu/research/hcrp/privacy/statereport> (accessed Sept. 5, 2002).
23. See, e.g., 42 C.F.R. § 482.24(b)(3) (2001).
24. *Id.* (references in regulation to "copies" and "original medical records" suggest applicability only to paper records).
25. 5 U.S.C. § 552a (2001) (regulating use of personal information held by federal agencies).
26. 42 U.S.C. § 12112(d)(3)-(4) (2001) (requiring that employers keep employees' medical records confidential).
27. Administrative Simplification Act, 110 Stat. at 2021-33.
28. *Id.* at 1936.
29. *Id.* at 2033.
30. 65 Fed. Reg. at 82,470.
31. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (1999).
32. 65 Fed. Reg. at 53,182.
33. 65 Fed. Reg. at 82,462.
34. See 67 Fed. Reg. at 53,182-183.
35. 67 Fed. Reg. at 53,182; U.S. Dept. of Health & Human Servs., *supra* note 1, at 2.
36. 65 Fed. Reg. at 53,183.
37. *Id.*
38. 67 Fed. Reg. at 53,182.
39. 42 U.S.C. § 1320d-4 (2002); 45 C.F.R. § 164.534.
40. 45 C.F.R. § 164.103.
41. 45 C.F.R. § 160.103.
42. See 42 U.S.C. § 1861(u) (2001); 65 Fed. Reg. at 82,477-82,478.
43. 65 Fed. Reg. at 82,469.
44. See 45 C.F.R. § 160.102.
45. See 45 C.F.R. § 164.501.
46. See 45 C.F.R. § 160.102.
47. 65 Fed. Reg. 82,488.
48. See *id.*
49. See 65 Fed. Reg. at 82,488.
50. See 45 C.F.R. § 164.501.
51. 45 C.F.R. § 164.502.
52. 45 C.F.R. § 164.514(a), (b).
53. 45 C.F.R. § 164.514(b)(1).
54. 45 C.F.R. § 164.514(b)(2).
55. 45 C.F.R. § 164.514(c).
56. See 45 C.F.R. § 164.502.
57. See 45 C.F.R. § 164.506(a).
58. See 45 C.F.R. § 164.501; 67 Fed. Reg. at 53,208.
59. See 45 C.F.R. § 164.501; 67 Fed. Reg. at 53,208.
60. 45 C.F.R. § 164.502(a)(1)(i).
61. 45 C.F.R. § 164.502(a)(1)(ii).
62. Other than inmates. See 45 C.F.R. § 164.520(a)(3).
63. 45 C.F.R. § 164.520(b)(1)(ii)(A).
64. 45 C.F.R. § 164.520(c)(2)(1)(A).
65. 45 C.F.R. § 164.520(c)(2)(1)(B).
66. 45 C.F.R. § 164.506(b).
67. See 67 Fed. Reg. at 53211, 53,241-53,242.
68. 45 C.F.R. § 164.520(c)(2)(ii). See 67 Fed. Reg. at 53,238-53,243.
69. 67 Fed. Reg. at 53,238-39, 53,240.
70. *Id.*
71. *Id.* at 53,239.
72. *Id.* at 53,240-53,241.
73. See 45 C.F.R. § 164.520(c)(2)(ii).
74. 67 Fed. Reg. at 53,193.
75. *Id.*
76. 45 C.F.R. § 164.502(a)(1)(iii).
77. See 67 Fed. Reg. at 53,193.
78. 45 C.F.R. § 164.508(a)(1).
79. 45 C.F.R. § 164.508(c)(3).
80. 45 C.F.R. § 164.508(c)(1).
81. 45 C.F.R. § 164.508(c)(2).
82. 45 C.F.R. § 164.508(b)(2)(iii).
83. 45 C.F.R. § 165.508(b)(2)(i).
84. 45 C.F.R. § 164.508(b)(2)(v).
85. 45 C.F.R. § 164.508(b)(2)(ii).
86. 45 C.F.R. § 164.508(b)(4).
87. 45 C.F.R. § 164.508(b)(4)(i).
88. 45 C.F.R. § 164.508(b)(4)(ii).
89. 45 C.F.R. § 164.508(b)(3).
90. 45 C.F.R. § 164.508(b)(3)(i), (ii).
91. 45 C.F.R. § 164.508(b)(3)(iii).
92. 45 C.F.R. § 164.508(b)(5).
93. 45 C.F.R. § 164.508(c)(4).
94. 45 C.F.R. § 164.502(b)(1).
95. 45 C.F.R. § 164.508(b)(2)(i).
96. 45 C.F.R. § 164.502(b)(2)(iii).
97. 45 C.F.R. § 165.502(b)(2)(iv). See also 45 C.F.R. § 164.512(1); 67 Fed. Reg. 53,198-199.
98. 45 C.F.R. § 164.502(b)(2)(iii).
99. 45 C.F.R. § 164.501.
100. *Id.*
101. See 67 Fed. Reg. at 53,185-86.
102. 45 C.F.R. § 164.502(e)(1). See 45 C.F.R. § 164.524(e)(1)(iii).
103. 45 C.F.R. § 160.103.
104. 45 C.F.R. § 164.512(j)(1)(ii).
105. 45 C.F.R. § 164.512(c).
106. 45 C.F.R. § 164.512(f)(2).
107. American Civil Liberties Union, *supra* note 7, at 1.
108. 45 C.F.R. § 164.512(b).
109. 45 C.F.R. § 164.512(b)(1)(iv).
110. 45 C.F.R. § 164.524(a)(1).
111. 45 C.F.R. § 164.524(b)(2)(i). See 45 C.F.R. § 164.524(b)(2).
112. 45 C.F.R. § 164.524(b)(2)(B)(ii).
113. 45 C.F.R. § 164.524(a)(1)(i). See 45 C.F.R. § 164.524(a)(1)(ii).
114. 45 C.F.R. § 164.524(a)(1)(iii). See 42 U.S.C. § 263a (2002); 42 C.F.R. § 493.3(a)(2) (2002).
115. See 67 Fed. Reg. at 53,200.
116. *Id.* See also 45 C.F.R. § 164.502(g)(3)(ii).
117. 45 C.F.R. § 164.512(j)(1)(i)(A). See also 67 Fed. Reg. at 53,200.
118. 45 C.F.R. § 164.528(a)(1)(i). See 67 Fed. Reg. at 53,243.
119. 45 C.F.R. § 164.528(a)(1)(v).
120. 45 C.F.R. § 164.528(b)(1). See 67 Fed. Reg. at 53,243.
121. 45 C.F.R. § 164.528(b)(1)(i).

122. 45 C.F.R. § 164.528(b)(1)(ii).
123. 45 C.F.R. § 164.528(b)(2)(iv)). *See also id.*
124. 45 C.F.R. § 164.512(b).
125. 45 C.F.R. § 164.528(b)(4).
126. 45 C.F.R. § 164.526(b)(1), (b)(2). *See* 45 C.F.R. § 164.526(a)(2)(iv) and 45 C.F.R. § 164.526(a)(1)(i).
127. 45 C.F.R. § 164.526(d).
128. 45 C.F.R. § 164.530(d)(2).
129. 45 C.F.R. § 164.530(j)(1)(ii). *See* 45 C.F.R. § 164.530(b)(2)(C)(ii) and 45 C.F.R. § 164.530(a)(1), (2).
130. 45 C.F.R. § 164.530(i)(1).
131. 45 C.F.R. § 164.530(i)(3).
132. 45 C.F.R. § 164.530(e)(2).
133. 45 C.F.R. § 164.530(j)(2).
134. 45 C.F.R. § 160.310(a).
135. 42 U.S.C. § 1320d-5, -6 (2002).
136. 42 U.S.C. § 1320d-6.
137. *See* Institute for Health Freedom, *supra*, note 9.
138. 45 C.F.R. § 160.306
139. 45 C.F.R. § 160.306(c).
140. 45 C.F.R. § 164.502(a)(2)(ii).
141. *See* Institute for Health Freedom, *supra*, note 9.
142. *See id.*
143. *See* 42 U.S.C. § 1320d-5, -6.
144. *See* U.S. Dept. of Health & Human Servs., *supra* note 1, at 1.
145. 45 C.F.R. § 160.203(b).
146. *See* 65 Fed. Reg. at 82,464.
147. *See* Health Privacy Project, *supra* note 9.
148. *See id.*
149. Confidentiality of Health Care Communications and Information Act, R.I. Gen. Laws § 5-37.3-4 (2001).
150. 45 C.F.R. § 164.512(a). *See also* 42 U.S.C. § 1320d-7(b) (2002).
151. 42 U.S.C. § 1320d-7 (2002); 45 C.F.R. § 160.203(c). *See* 65 Fed. Reg. at 82,485. *See also* 42 U.S.C. § 1320d-7(b) (2002).
152. *See* 65 Fed. Reg. at 82,485.
153. *See id.*
154. *See* 45 C.F.R. § 164.103.
155. *See* 45 C.F.R. § 164.501.
156. *See id.*
157. *See id.* *See also* 20 U.S.C. § 1232g (2000).
158. 45 C.F.R. § 164.514(b)(2)(i).
159. 45 C.F.R. § 164.514(b)(2)(ii).
160. 45 C.F.R. § 164.520(b)(1).
161. *See* 45 C.F.R. § 164.520(b)(1)(iii).

162. *See* 45 C.F.R. § 164.520(c)(3)(ii).
163. *See* 45 C.F.R. § 164.520(c)(3)(i).
164. 45 C.F.R. § 164.508(c)(1).
165. 45 C.F.R. § 164.508(c)(2).
166. 45 C.F.R. § 164.508(b)(1)(ii).

CE/CME Questions

17. The Privacy Rule applies to which of the following?
 - A. All health information
 - B. Personal health information
 - C. Individually identifiable health information used or disclosed by entities that utilize electronic information technology
 - D. All disclosures of health information to the public

18. Which of the following is true?
 - A. State privacy laws have been replaced entirely by the Privacy Rule.
 - B. The Privacy Rule preempts contrary provisions of state law, except where statutory provisions are more stringent.
 - C. State privacy laws enacted before the Privacy Rule supercede the Privacy Rule.
 - D. State privacy laws have not been affected by the Privacy Rule.

19. The Privacy Rule allows an ED nurse to disclose the health information of a patient, without the patient's prior authorization, under which of the following circumstances?
 - A. An official of the FDA needs the information to contact a patient who has been prescribed a harmful medication.
 - B. A police officer demonstrates that the information is necessary to save another person's life.
 - C. The nurse believes that the patient would benefit by

CE/CME Objectives

[For information on subscribing to the CE/CME program, contact customer service at (800) 688-2421 or e-mail customerservice@ahcpub.com.]

The participants will be able to:

- identify high-risk patients and use tips from the program to minimize the risk of patient injury and medical malpractice exposure;
- identify a "standard of care" for treating particular conditions covered in the newsletter;
- identify cases in which informed consent is required;
- identify cases which include reporting requirements;
- discuss ways in which to minimize risk in the ED setting.

ED Legal Letter was saddened by the death of longtime editorial board member **James Zimmerly, MD, JD, MPH, LLD, FCLM**, who died in October.

Attending law school at night while completing residency, Dr. Zimmerly was a pioneer in the field of legal medicine. He convinced his superiors in the military that there was a need for a legal medicine department, and developed the Department of Legal Medicine at the Armed Forces Institute of Pathology, Walter Reed Hospital.

His many accomplishments included co-discovery of the meningococcal meningitis vaccine, which he tested on himself prior to vaccinating military personnel. He was an accomplished legal writer and editor. His contributions to the field of legal medicine will be greatly missed.

receiving brochures from a pharmaceutical company about a new drug.

D. Both A and B are allowable.

20. Which of the following activities is prohibited under the Privacy Rule?
- A. Calling out the name of a patient in an ED waiting room
 - B. Requiring patients to sign in while waiting for triage
 - C. Transmitting protected health information by e-mail
 - D. Routinely denying patients access to their medical records

Audio Conference Tackles HIPAA Privacy Concerns

The recently released final privacy rule under the Health Insurance Portability and Accountability Act (HIPAA) makes significant changes to the existing regulations. With the April 14, 2003, compliance deadline fast approaching, is your staff receiving the proper training?

The American Hospital Association says implementing HIPAA will require “sweeping operational changes” and will take “intense education of hospital workers and patients.” To help you and your staff prepare, American Health Consultants offers *HIPAA’s Final Privacy Regulations: What You Must Know to Comply*, an hour-long audio conference on **Dec. 4, 2002, from 2:30-3:30 p.m. ET**. You’ll learn detailed information on changes to the privacy rule, as well as practical methods to implement new procedures within your facility. Do you know what your enforcement priorities are? Do you need real-world examples? Our expert speakers, **Debra Mikels** and **Chris Wierz, BSN, MBA**, will help you understand your responsibilities and identify potential liabilities. All this will allow you to develop a HIPAA compliance strategy with a rationale behind it.

Mikels is corporate manager, confidentiality, for Partners Healthcare in Boston. The Partners system includes some of the largest and most respected facilities in the country, including Massachusetts General Hospital, Brigham and Women’s Hospital, and Harvard Medical School.

Wierz is vice president of HIPAA and compliance initiatives for Houston-based Healthlink Inc., a health care consulting firm. She has worked with numerous facilities across the country to prepare them for HIPAA compliance, and now she shares many of her ideas with you.

The cost of the conference is \$299, which includes free CE or CME for your entire staff, program handouts, and additional reading, a convenient 48-hour replay, and a conference CD. Don’t miss out. Educate your entire facility for one low price.

For more information or to register for the HIPAA audio conference, please call American Health Consultants’ customer service department at **(800) 688-2421**. When ordering, please refer to effort code: **65151**.

In Future Issues:

Asset Protection

United States Postal Service
Biometrics for Ownership, Management and Circulation

1. Title of Publication: **Journal of the American Medical Association**

2. Issue Frequency: **Weekly**

3. Complete Mailing Address of Known Office of Publication (Not printer): **5255 Woodmont Road, N.W., Atlanta, GA 30328**

4. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer): **5255 Woodmont Road, N.W., Atlanta, GA 30328**

5. Complete Mailing Address of the Publisher: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

6. Complete Mailing Address of the Circulation Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

7. Complete Mailing Address of the Advertising Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

8. Complete Mailing Address of the Distribution Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

9. Complete Mailing Address of the Subscription Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

10. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

11. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

12. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

13. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

14. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

15. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

16. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

17. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

18. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

19. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

20. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

21. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

22. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

23. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

24. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

25. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

26. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

27. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

28. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

29. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

30. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

31. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

32. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

33. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

34. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

35. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

36. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

37. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

38. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

39. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

40. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

41. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

42. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

43. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

44. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

45. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

46. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

47. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

48. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

49. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

50. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

51. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

52. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

53. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

54. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

55. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

56. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

57. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

58. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

59. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

60. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

61. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

62. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

63. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

64. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

65. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

66. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

67. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

68. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

69. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

70. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

71. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

72. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

73. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

74. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

75. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

76. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

77. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

78. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

79. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

80. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

81. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

82. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

83. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

84. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

85. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

86. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

87. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

88. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

89. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

90. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

91. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

92. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

93. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

94. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

95. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

96. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

97. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

98. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

99. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

100. Complete Mailing Address of the Fulfillment Office: **5255 Woodmont Road, N.W., Atlanta, GA 30328**

Insert. Strategies for Coping with the Privacy Rule

Implementation of the Privacy Rule will change the way America's health care providers do business. The following strategies will help EDs make the smoothest transition possible:

1. KNOW THE RULE.

EDs cannot comply with the Privacy Rule unless their administrators and personnel understand the rule's requirements. This article highlights only those provisions most relevant to ED practice. ED administrators and practitioners should consult with their attorney before the compliance date to discuss all of the ways in which their ED practices will be affected.

2. ADOPT APPROPRIATE POLICIES.

Do not assume that the personnel in your ED understand their responsibilities with regard to health information, or even that they have heard of HIPAA. Guide them with appropriate policies.

3. PROVIDE ADEQUATE TRAINING.

ED personnel do not always devote sufficient attention to hospital policies and memos, no matter how well these documents have been drafted. Reinforce these measures with face-to-face training sessions. In fact, the Privacy Rule mandates such training.

4. DESIGNATE AN ED COMPLIANCE OFFICER AND A CONTACT PERSON FOR PRIVACY-RELATED ISSUES.

The Privacy Rule requires these appointments, but they also make sense. EDs can no longer police themselves on privacy matters. The regulations are too complicated, and the potential for liability is too great. This is an area that deserves expert oversight.

5. TAKE STEPS TO COMPLY NOW.

Privacy Rule compliance will require the implementation of training programs, adoption of new policies, renegotiation of contracts, and the drafting

of authorization and notice forms. These activities cannot occur overnight, and last-minute decision making will lead to mistakes and liability. Begin the compliance process now.

6. SEEK CONSENT.

The Privacy Rule does not require health care providers to obtain consent for uses and disclosures of protected health information. Doing so may prove useful in avoiding legal problems, however.

7. RESPECT STATE LAW.

Remember that state privacy laws may impose duties beyond those created by the Privacy Rule. Make sure that your ED policies reflect this fact.

8. UTILIZE HHS RESOURCES.

HHS's Office for Civil Rights (OCR) provides guidance in complying with the Privacy Rule. Contact OCR directly with questions, or visit the OCR website at <http://www.hhs.gov/ocr/hipaa>.

9. WATCH FOR CHANGES.

The final version of the Privacy Rule may not be final after all. The chairman of the Senate Health Committee, Sen. Edward Kennedy (D-Mass), announced in August that he would seek additional Privacy Rule changes through the legislative process.¹ Medical and civil rights groups are considering a lawsuit to modify some of the rule's provisions.² ED administrators should remain alert for changes in the Privacy Rule's status, and be prepared to respond appropriately.

Endnotes

1. Amy Goldstein, *HHS Issues Privacy Rules for Use of Health Records*, Washington Post, Aug. 10, 2002, at A1. See 67 Fed. Reg. 53,185-90 (2002).
2. See *id.*