

## N.J. Plan Requires Too Much PHI For Payment, Psychologists Allege

The amount and type of protected health information (PHI) being required as a condition of payment by a group health plan's administrator and managed behavioral health vendor is being challenged in court by two plan participants and a state psychologists' group.

The lawsuit, filed by the New Jersey Psychological Association and two participants in the state government's group health plan, alleges that Horizon Healthcare Services, Inc. and Magellan Healthcare Services, Inc. violated the HIPAA privacy requirements incorporated into the plan documents, as well as New Jersey's psychologist-patient privilege law.

Horizon and Magellan allegedly violated HIPAA's minimum necessary standard by "requesting confidential communications between psychologists and patients," without adequate justification, "in connection with initial and continuing treatment authorization (and consequently) payment determinations." *Page 2*

## Patient's Entire EMR May Be Used To Defend Malpractice Lawsuit

By suing a doctor, group practice and HMO for malpractice, a patient waived his state-law privileges for his entire electronic medical record (EMR), the Colorado Supreme Court ruled by a 6-1 vote.

In Colorado, when a patient sues a physician over his or her treatment, "the physician may be examined as to any information acquired in attending the patient that was necessary to enable the physician to prescribe or act for the patient." Because the HMO has a complete EMR on each member, when one of its physicians treats a patient, "he necessarily acquires the entire medical record," the majority ruled. Therefore, Ortega's entire EMR "is not protected by the physician-patient privilege."

The dissent, however, argued that just "because a patient happens to belong to an HMO that maintains an integrated [EMR] system" should not mean he gives up the privilege for his nearly 700 records stored there, of which the "vast majority" are totally unrelated to his lawsuit. *Page 3*

## First 20 HIPAA Audits Under Way

Group health plans are among the first 20 HIPAA-covered entities that are now being audited for HIPAA privacy and security compliance. The 20 health plans and providers selected for this "initial wave" by the U.S. Department of Health and Human Services are spread across four "levels" of size and sophistication. *Page 4*

### Also In This Issue

Final Medicare Data Rules Offer More Flexibility.....	4
Massive Calif. Provider Breach Triggers Lawsuit.....	5
Operating Rules to Take Effect as Issued In July.....	6
GINA Allows Asking Reason for 401(k) Hardship Loan.....	6
Subject Index.....	7

### Editor's Note

Please file this monthly newsletter behind the "Current Developments" or "Newsletters" tab in your looseleaf manual. Your next quarterly update to the *Guide* will be mailed to you in February.

### Webinar Alert

**Jan. 10:** Employee Record Retention

**Jan. 18:** Creating Bulletproof Documentation

**Jan. 19:** Cafeteria Plan and FSA Rules: A 'To Do' List for 2012

**Jan. 25:** Form 5500 — Stay Compliant and Penalty-free

**Jan. 31:** Avoiding Common COBRA Compliance Mistakes

**Feb. 2:** Correct Reporting and Tax Treatment Of Fringe Benefits

**Feb. 15:** Self-Insured Health Plans: New Legislative and Regulatory Developments

Go to <http://www.thompsoninteractive.com> for a complete list of upcoming webinars and other audio conferences.

### Contact Us

Customer Service: 800 677-3789

Online: [www.thompson.com](http://www.thompson.com)

Editorial: 202 872-4000

## N.J. Employee Plan's Administrator Requires Too Much PHI for Payment, Psychologists Allege

The amount and type of protected health information (PHI) being required as a condition of payment by a group health plan's administrator and managed behavioral health vendor is being challenged in court by two plan participants and a state psychologists' group.

The lawsuit, filed by the New Jersey Psychological Association (NJPA) and two participants in the state government's group health plan (NJ Direct), alleges that Horizon Healthcare Services, Inc. and Magellan Healthcare Services, Inc. violated the HIPAA privacy requirements incorporated into the plan documents, as well as New Jersey's psychologist-patient privilege law.

"They put us between a rock and a hard place by requiring psychologists to violate patient confidentiality and disclosing patients' innermost thoughts and feelings or denying authorization that limits patients' access to care," said NJPA President Sharon Ryan Montgomery.

According to the lawsuit, Horizon and Magellan breached the plan documents and violated HIPAA's minimum necessary standard by "requesting confidential communications between psychologists and patients in connection with initial and continuing treatment

authorization (and consequently) payment determinations." These demands allegedly were made without "legitimate justification" simply to discourage psychological treatment or reduce mental health coverage.

HIPAA's privacy rules allow PHI disclosure for treatment, payment and health care operations (TPO) (see ¶210 of the *Guide*), but disclosures for payment or health care operations generally must be limited to the minimum PHI necessary (see ¶311). To support their interpretation of minimum necessary, NJPA and the other plaintiffs cited a standard "treatment request form" that Magellan requires psychologists to complete for treatment approval. The form was drafted to comply with a New Jersey law's restrictions on the information psychologists may disclose to private payers.

Although this law does not apply to NJ Direct, Magellan's use of the form for all plans "demonstrates that Magellan is able to make treatment authorization determinations" from this limited information, "whether the patient is covered under a private insurance plan or a government-sponsored plan," NJPA argues.

Such decisions "can be (and in the past were) made by Defendants based upon the minimum necessary information, such as the dates of requested service, the primary diagnostic code and the Current Procedural Terminology code," according to the lawsuit. "None of this information seeks confidential psychologist-patient communications revealing the innermost thoughts and feelings."

But in the NJ Direct plan, Horizon and Magellan now go well beyond this as a standard practice, NJPA alleges. "For example, Magellan has medical necessity guidelines that seek excessive information unnecessary for making treatment decisions," according to the lawsuit. This includes "a psychologist's treatment notes regarding a patient's information as to the presence of familial support or reasons for the lack of familial support, and details regarding a patient's specific symptoms and issues."

HIPAA does not provide a private right to sue (see ¶630), but does require certain privacy provisions to be included in the plan documents (see ¶323), which in turn can form the basis for an ERISA lawsuit (or, in the case of a non-ERISA plan like NJ Direct, a lawsuit under state contract law).

Along with minimum necessary, NJPA's lawsuit cited HIPAA's special protections for "psychotherapy notes"

### Employer's Guide to HIPAA Privacy Requirements

CONTRIBUTING EDITORS: **KATHY BAKICH, Esq.**

**JOANNE HUSTEAD, Esq.**

THE SEGAL COMPANY

DIRECTOR OF PUBLISHING: **LUIS HERNANDEZ**

ASSOCIATE PUBLISHER: **GWEN COFIELD**

EDITOR: **DAVID A. SLAUGHTER**

CONTRIBUTING WRITER: **MARA CHERKASKY**

PRODUCTION MANAGER: **JASON B. PEACO**

The *Employer's Guide to HIPAA Privacy Requirements* (USPS 021-082) is published monthly with quarterly updates by Thompson Publishing Group, 805 15th St. NW, 3rd Floor, Washington, DC 20005. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. ISSN: 1543-5873

POSTMASTER: Send address changes to: *Employer's Guide to HIPAA Privacy Requirements*, Thompson Publishing Group, 5201 W. Kennedy Blvd., Suite 215, Tampa, FL 33609-1823.

This newsletter for the *Employer's Guide to HIPAA Privacy Requirements* includes a looseleaf update to the *Guide*. For subscription service, call 800 677-3789. For editorial information, call 202 872-4000. Please allow four to six weeks for all address changes.

This information is designed to be accurate and authoritative, but the publisher is not rendering legal, accounting or other professional services. If legal or other expert advice is desired, retain the services of an appropriate professional.

Copyright ©2012 by Thompson Publishing Group.

 **THOMPSON**  
Insight you trust.

See *N.J. Plan*, p. 5

# Patient's Entire EMR May Be Used to Defend Malpractice Lawsuit, Colorado Supreme Court Rules

By suing a doctor, group practice and HMO for malpractice, a patient waived his state-law privileges for his entire electronic medical record (EMR), the Colorado Supreme Court ruled by a 6-1 vote. The case is *Ortega v. Colo. Permanente Group, P.C.*, 2011 WL 5325518 (Colo., Nov. 7, 2011).

## Facts of the Case

Ernest Ortega, a member of the Kaiser Foundation Health Plan of Colorado, sought treatment from Dr. David Lieuwen, his primary care physician, for pain in his chest, neck, shoulders and back. Lieuwen gave Ortega a treadmill stress test and then discharged him, but he suffered a heart attack on the way to his car. Ortega sued Kaiser, Lieuwen and his group practice for negligence, claiming “broad and numerous damages.”

Since 1998, Kaiser has kept EMRs that enable treating providers to access a patient’s entire electronic medical history. The EMR on Ortega, a longtime Kaiser participant and patient, consisted of nearly 700 different records. When he filed suit, Ortega compiled a “privilege log” of documents he claimed were privileged because they did not relate to the circumstances surrounding the lawsuit. (HIPAA’s privacy rules did not come into play because Ortega conceded that Colorado’s privilege is more stringent than federal laws, and HIPAA expressly preserves stricter state privacy laws (see ¶811 of the *Guide*.)

Ortega asked the trial court for a protective order to prevent the defendants from reviewing the EMR, but the court refused, finding that the entire EMR was exempt from the physician-patient privilege. Since disclosure is not something that can be undone in the normal judicial appeals process, the Colorado Supreme Court agreed to hear Ortega’s appeal immediately before the case proceeded further.

## Majority Opinion

Most states have physician-patient privilege laws, which generally include exceptions enabling physicians to use a patient’s records in their defense if that patient sues them. Colorado’s privilege has an exception stating that when a patient sues a physician over his or her treatment, “the physician may be examined as to any information acquired in attending the patient

that was necessary to enable the physician to prescribe or act for the patient.”

Kaiser providers have “a complete electronic medical record for each member,” so when one treats a patient, “he necessarily acquires the entire medical record,” Justice Nancy Rice wrote for the majority. Therefore, Ortega’s entire EMR “is not protected by the physician-patient privilege.”

Kaiser itself, as an HMO, is subject to a different state law, but the court found that a similar exception applied. HMOs generally may not disclose enrollees’ health information, but the law includes an exception “in the event of claim or litigation” between the HMO and enrollee “wherein such data or information is pertinent,” Rice noted. Thus, the HMO law “permits Kaiser to examine Ortega’s [EMR], to the extent the record is relevant to claims raised by Ortega against Kaiser, because Ortega brought suit against Kaiser.”

The majority therefore upheld the trial court’s ruling that the defendants could examine unredacted copies of Ortega’s entire EMR because it was relevant. “A review of Ortega’s medical record is relevant to enable defendants to prepare an answer, assert defenses, develop legal theories, plan discovery, and determine evidence and witnesses for trial,” Rice explained. This does not mean that the entire record can actually be used as *evidence* at trial, because Ortega still may object to the admission into evidence of specific information that might be “unrelated or irrelevant” for these purposes.

See *EMR*, p. 7

## Editorial Advisory Board

### KATHRYN BAKICH, ESQ.

The Segal Company  
Washington, D.C.

### RICH GLASS, J.D.

Infinisource, Inc.  
Dallas

### PAUL M. HAMBURGER, ESQ.

Proskauer Rose LLP  
Washington, D.C.

### JACK B. HELITZER, ESQ.

Fairfax, Va.

### TERRY HUMO, ESQ.

Missoula, Mont.

### JOANNE HUSTEAD, ESQ.

The Segal Company  
Washington, D.C.

### MARK E. LUTES, ESQ.

Epstein Becker & Green, P.C.  
Washington, D.C.

### JOSEPH A. MURPHY, JR., ESQ.

Washington, D.C.

### JON A. NEIDITZ, ESQ.

Nelson Mullins Riley & Scarborough LLP  
Atlanta

### LYNDA M. NOGGLE, ESQ.

Proskauer Rose LLP  
Washington, D.C.

### GEORGE PANTOS, ESQ.

WellNet Healthcare  
Bethesda, Md.

### ADAM RUSSO, ESQ.

Russo & Minchoff LLP  
Boston

### MARK L. STEMBER, ESQ.

Kilpatrick Townsend & Stockton LLP  
Washington, D.C.

### ROBERTA CASPER WATSON, ESQ.

Trenam Kemker  
Tampa, Fla.

# First 20 HIPAA Privacy Audits Under Way

Group health plans are among the first 20 HIPAA-covered entities that are now being audited for HIPAA privacy and security compliance. The 20 health plans and providers selected for this “initial wave” by the U.S. Department of Health and Human Services (HHS) are spread across four “levels” of size and sophistication.


“The first 20 audit letters have been sent to covered entities,” according to an official with HHS’ Office for Civil Rights (OCR). These entities also receive document requests from KPMG LLP, HHS’ audit contractor, and must provide the requested documents within 10 days (see December 2011 newsletter).

“The OCR notification letter will introduce the audit contractor, explain the audit process and expectations in more detail, and describe initial document and information requests,” the agency indicated on its website. “It will also specify how and when to return the requested information to the auditor.”

The 20 recipients consist of 10 health care providers, two health care clearinghouses and eight health plans, which in turn include three group health plans, according to former OCR official Adam Greene, now an attorney with Davis Wright Tremaine LLP. One is classified as a “Level 3” (out of four) covered entity, and the other two are Level 4, Greene reported on the firm’s website.

“The level classifications are general categorizations to assist OCR and KPMG with planning resource needs for audits. Level 4’s generally have revenues of \$50 million or less,” according to a statement OCR provided to the *Guide*. “These original tiers are likely to change with experience.”

## For More Information

Details of the audit program are now available on OCR’s website at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit>. 

---

# Final Medicare Data Rules Offer More Flexibility


Final rules governing the release of Medicare claims data for quality measurement include changes from the proposed version designed to make it easier for would-be recipients to qualify. However, the data privacy and security provisions were made even more stringent, and health care providers were given more opportunity to review and appeal performance reports before they are released to the public.

Under the final rules issued Dec. 7 (76 Fed. Reg. 76542) by the Centers for Medicare and Medicaid Services (CMS), the claims information will be released only to organizations that meet numerous requirements, involving privacy and security as well as methodology and inclusion of private plan data. Employers and consumer groups are among the “qualified entities” that CMS expects will participate in the program, which was mandated by the health reform law.

The final rules include many changes from the version CMS proposed in June (see August 2011 newsletter). The revisions will make the data less costly for qualified entities and give them more flexibility in using it to create performance reports for consumers, but also extend the time period for health care providers to review and appeal reports before their release, CMS stated. Releasing any information on individual beneficiaries would be prohibited and subject to civil and criminal penalties.

CMS’ rules should help employers and individuals alike make more informed decisions down the road, advancing the goals of health care quality and value, a plan sponsor representative noted — especially since qualifying data recipients will be allowed to analyze this information on a provider-specific basis. “Having that transparency allows you to go to the next step — payment methodologies that are based on quality, and ultimately value,” said Kathryn Wilber of the American Benefits Council.

In the past, employers, consumers and others have been frustrated by “the limited and piecemeal availability of Medicare data that could be used to help evaluate health care provider or supplier performance,” according to CMS’ statement. Many health plans have created their own performance reports but “these reports are based solely on the health plans’ own claims, and do not reflect information from other health plans, including Medicare.”

The final rules include a conditional approval process for applicants that do not have access to claims data from other sources at the time of their application. An entity also may contract with others to apply jointly, if necessary to meet all the eligibility criteria. Applicants must have “a rigorous data privacy and security program” and disclose any past “inappropriate disclosures of beneficiary identifiable information” or violations of privacy or security laws. (The proposed rules had referenced only HIPAA violations.) 

# Massive Calif. Provider Breach Triggers Lawsuit

Yet another simple laptop theft has resulted in a massive data breach and a class-action lawsuit. California's Sutter Health, it is alleged, negligently failed to secure the personal information on more than 3 million patients that was stored unencrypted on a computer stolen from the organization's Sacramento headquarters.


By failing to "safeguard and secure its patients' private information," Sutter Health violated California's Confidentiality of Medical Information Act, which requires providers and other business entities to keep medical records confidential, according to the complaint filed by Dreyer, Babich, Buccola & Wood LLP on behalf of a Sutter patient and similarly situated individuals.

Sutter Health President and CEO Pat Fry expressed regret about the breach. "The Sutter Health Data Security Office was in the process of encrypting computers

throughout our system when the theft occurred, and we have accelerated these efforts," according to his Nov. 16 statement.

## Study Shows Rise in Breaches

The number of health care data breaches is still increasing, and many health care organizations believe they lack the funds needed to fully ensure the privacy and security of protected health information, a recent study indicates.

The percent of organizations reporting zero breaches dropped from 14 percent to 4 percent between 2010 and 2011, and the percentage of organizations reporting more than five breaches rose from 29 percent to 46 percent, according to the Ponemon Institute's *Second Annual Benchmark Study on Patient Privacy and Data Security*, sponsored by security firm ID Experts (see <http://www2.idexpertscorp.com>). 

## N.J. Plan (continued from page 2)

as "further support for the impropriety of Defendants' request." In general, psychotherapy notes may not be disclosed without an individual's written authorization, even if the disclosure is for TPO purposes.

The U.S. Department of Health and Human Services (HHS) defined psychotherapy notes to exclude information such as treatment "modalities and frequencies," test results, counseling times, prescriptions and certain summary diagnostic data (see ¶221). These specific exceptions, NJPA argued, "provide further guidance on the minimum necessary information."

The lawsuit asks the state court to declare that Horizon and Magellan violated the plan documents and the state privilege law, and "grant such other and further relief as may be just and proper."

## Companies' Response

Horizon and Magellan deny having done anything improper or overly intrusive. "The information requested from providers by Magellan is entirely appropriate and consistent with applicable federal and state laws," and with the plan provisions requiring Horizon and Magellan "to ensure treatment meets the medical necessity requirements of the Program," according to a joint statement.


Horizon and Magellan "respect the confidentiality rights of our members," but nothing in the plan documents or the laws cited by NJPA "changes the member's obligation to satisfy medical necessity requirements for coverage," the companies said.

## Implications

HIPAA's lack of a private right to sue has forced litigants to be creative in finding ways to accomplish indirectly what cannot be done directly. This lawsuit cites HIPAA privacy compliance as a contractual obligation in a breach-of-contract case where the underlying contract is the group health plan's plan document.

The NJ Direct Member Handbook, cited as the relevant plan document, referred to the minimum necessary standard and thus provided the foundation for the alleged breach of contract. While HIPAA's privacy rules do require the plan documents to include certain statements, including the plan sponsor's permitted uses and disclosures (see ¶560), it is not required to include the entire privacy notice, as NJ Direct apparently did.

The central issue that must be resolved is the amount of detail that Magellan actually needs to determine whether certain mental health claims should be paid. HIPAA's minimum necessary standard is very general and applying it to particular circumstances is not always an easy task (see ¶311). The special status HIPAA accords psychotherapy notes could help the court draw clear lines.

Section 13405(b) of the Health Information Technology for Economic and Clinical Health (HITECH) Act requires HHS to provide guidance on the minimum necessary standard. In the preamble to its July 2010 proposed HITECH rules, the agency solicited comments on what this guidance should include, but has yet to issue it. 

Get the latest HR news and analysis from our new blog! Visit [SmartHRManager.com](http://SmartHRManager.com).

# Operating Rules to Take Effect as Issued in July

The elaborate operating rules that the U.S. Department of Health and Human Services (HHS) issued last July in interim final form will take effect without modifications, HHS' Centers for Medicare and Medicaid Services (CMS) announced Dec. 7.

These regulations, which codify detailed uniform procedures for performing HIPAA's eligibility and claims status transactions, are "a final rule that is in effect now, which means industry implementation efforts should be underway for the January 1, 2013 compliance date," according to a notice CMS posted on its website. Plans will be required to certify compliance by the end of 2013 or face substantial penalties (see April 2011 newsletter).

CMS had indicated, in its July 8 "interim final rule with comment period" (IFC) (76 Fed. Reg. 40458), that "if we received comments that compelled us to change any of the policies in the IFC, we would seek to finalize such changes by January 2012 to allow industry sufficient time to prepare for compliance," the agency explained. "After careful review and consideration of all the comments, we have decided not to change any of the policies established" by the rules.

The operating rules, the first of many mandated by the Patient Protection and Affordable Care Act (PPACA), were largely based on the voluntary operating rules already developed by the Committee for Affordable Quality Healthcare's Committee on Operating Rules for Information Exchange (CORE). Their goal is to harmonize the use of HIPAA's standard transactions and reduce the role of plan-specific "companion guides" (see ¶1010 of the *Guide*).

However, CMS did not adopt the certification process that CORE originally included in these operating rules. "We do not require covered entities to secure CORE certification or comply with any of the CORE certification policies," the agency reiterated in the notice.

The adopted rules' references to CORE certification, or acknowledgment standards, "may be accommodated voluntarily by covered entities and between willing trading partners, but are not required under HIPAA, nor subject to HIPAA enforcement actions," CMS added.

Covered entities may start using the operating rules before the Jan. 1, 2013, deadline, and HHS encourages them to do so "with willing trading partners, because of the benefits and efficiencies that can be enjoyed by both health plans and providers."


## NCVHS Seeks Clarity on Certification

A federal advisory committee called on HHS to prevent confusion over future operating rules by deleting references to CORE certification from any documents that the agency adopts as mandatory.

"The language in the operating rules that requires CORE Certification specifically can be misleading," according to the National Committee on Vital and Health Statistics (NCVHS). "We suggest that CAQH CORE certification be explicitly and separately noted as a voluntary option," but omitted from future operating rules.

HHS also should reclassify operating rules into "business" and "technical" rules, instead of the "phases" in which CORE originally developed the voluntary versions, CORE recommended: "Industry users would apply the technical rules across all transactions, and use the documents for each transaction to implement the business rules for that specific transaction."


### For More Information

CMS' notice can be found on the agency's website at <http://www.cms.gov/Affordable-Care-Act>. The full text of NCVHS' recommendations is available at <http://www.ncvhs.hhs.gov/111207lt.pdf>. 

## GINA Allows Asking Reason For 401(k) Hardship Loan

Asking a pension plan beneficiary why he or she needs a hardship loan from his or her 401(k) plan does not violate the Genetic Information Nondiscrimination Act (GINA), despite the possibility that the reason given will relate to a family member's health problem, staff attorneys for the U.S. Equal Employment Opportunity Commission (EEOC) indicated informally.

"Why do you need to make a hardship withdrawal?" is not a request for genetic information, "even if one of the possible responses is the need to pay medical expenses related to a genetic test or to the current health of an employee's family member," the EEOC staff told benefits attorneys.

This is not even a request for *medical* information, so "the staff would not expect hardship withdrawal forms to include the safe harbor language" normally required for accommodation requests under the Americans With Disabilities Act (see ¶723 of the *Guide*), the EEOC attorneys added. 

New edition of Health Care Reform book available! Go to [www.thompson.com/HCRL](http://www.thompson.com/HCRL)

**Dissenting Opinion**

Chief Justice Michael Bender dissented, arguing that just “because a patient happens to belong to an HMO that maintains an integrated [EMR] system” should not mean he gives up the privilege for his nearly 700 records stored there, of which the “vast majority” are totally unrelated to his lawsuit.

Specifically, Bender took issue with the majority’s finding that Lieuwen’s “access” to Ortega’s EMR meant he had “acquired” it so as to trigger the privilege exception. “There is no evidence that Dr. Lieuwen actually acquired or used all of Ortega’s medical records in his treatment of Ortega, only that he has access to the records in Kaiser’s system,” Bender wrote. “By failing to acknowledge this significant distinction, I suggest the majority misreads the mandate of the statute.

“Even if Dr. Lieuwen had actually acquired all of Ortega’s records,” Bender added, the criteria for the privilege exception still would not have been satisfied because few of them could have been “necessary” to treat Ortega:

In this case, there has been no showing that almost ten years of Ortega’s medical history, containing nearly 700 records, were necessary for Dr. Lieuwen to treat Ortega’s chest, neck, shoulder, and back pain. It is obvious that Dr. Lieuwen could not have possibly reviewed nearly 700 records during his brief treatment of Ortega.

It shouldn’t matter that Kaiser already possesses these records, Bender continued. “No matter who possesses the records, the privilege-holder — here, the patient — controls the privileged information and determines who may obtain access, absent a waiver,” he wrote. And determining to what extent a patient-plaintiff has waived the privilege requires going through the “privilege log” of specific records like the one Ortega submitted, rather than simply issuing “a blanket order requiring disclosure of all of Ortega’s medical records.”


**Plan Sponsor Implications**

HIPAA’s privacy rules would not have provided greater protection to this EMR than Colorado’s privilege laws, because of HIPAA’s broad definition of “health care operations” (see ¶215). This definition, which includes legal services regarding an entity’s “covered functions,” would allow a health care provider who is sued for malpractice to use the plaintiff-patient’s PHI in his possession (even an entire EMR) to prepare a defense to that lawsuit (see ¶342).

Storing these records in an EMR or other electronic database would make it easier for the provider to locate, compile and search them for potentially relevant information. But it could also help the patient, since HIPAA entitles individuals to a copy of their medical records in any form in which it is “readily producible,” and the Health Information Technology for Economic and Clinical Health (HITECH) Act creates a specific right to electronic access (see ¶431).

Litigation over whether an entire EMR may be accessed during discovery will likely become commonplace as more health care providers start using EMRs, as the HITECH Act’s monetary incentives encourage them to do. However, the majority’s broad holding that an entire EMR can be accessed is significant, as Chief Justice Bender stated in his dissent:

If all medical records become digitized, the majority’s holding may have the effect of requiring all plaintiffs to disclose their entire history of medical records if they bring a malpractice suit because all of the plaintiff’s physicians will have had access to all of the plaintiff’s private medical records.

Other workplace litigation, such as workers’ compensation or wrongful discharge, also could be implicated if access to EMRs is broadly defined, as in this case. 

**Subject Index • Volume 10**

This subject index covers the *Employer’s Guide to HIPAA Privacy Requirements* newsletter, Volume 10, Nos. 1-12. Entries are listed alphabetically by subject and the name of the court case. The numbers following each entry refer to the volume, issue number and page number of the newsletter in which information on that topic or case appeared. For example, the designation “10:1/2” indicates Vol. 10, No. 1, page 2.

**Index by Subject**

Access rights, 10:2/2, 10:10/4  
 Accounting of disclosures, 10:5/3, 10:6/3, 10:8/5  
 Americans With Disabilities Act, 10:4/6, 10:5/2, 10:8/7, 10:10/4, 10:11/4  
 Breach notification, 10:3/6, 10:4/2, 10:6/5, 10:8/6, 10:9/5, 10:10/2, 10:10/3, 10:10/6  
 Business associates, 10:9/2, 10:9/4, 10:10/2, 10:10/6, 10:11/2  
 Claims and appeals, 10:7/3  
 COBRA administration, 10:2/3  
 Disposal practices, 10:3/6

Get the latest HR news and analysis from our new blog! Visit [SmartHRManager.com](http://SmartHRManager.com).

## Subject Index • Volume 10 (continued)

Employee assistance programs, 10:5/4  
Employee sanctions, 10:2/5, 10:2/7  
Employment records, 10:2/3, 10:5/4  
Enforcement, 10:2/2, 10:2/7, 10:3/2, 10:3/4, 10:3/5, 10:7/5,  
10:9/5, 10:10/5, 10:11/2, 10:11/6  
Audits, 10:3/7, 10:8/2, 10:11/3, 10:12/4  
Criminal, 10:10/7  
EDI, 10:3/3  
Security, 10:5/3, 10:5/6  
State, 10:3/6, 10:8/6  
ERISA preemption, 10:4/3, 10:8/3  
Fair Credit Reporting Act, 10:7/6  
Federal Trade Commission, 10:1/3  
Genetic Information Nondiscrimination Act, 10:4/6, 10:8/7,  
10:10/4, 10:11/4, 10:12/6  
Group health plan disclosures, 10:6/5, 10:8/3, 10:10/6  
Health information technology, 10:1/4, 10:4/7, 10:5/7, 10:8/7,  
10:9/4, 10:12/3  
Litigation, PHI disclosure for, 10:4/4, 10:6/6, 10:6/7, 10:12/3  
Marketing, 10:1/2, 10:1/5, 10:3/4, 10:6/2  
Medicare data, 10:7/11, 10:12/4  
Mergers and acquisitions, 10:7/2  
Minimum necessary, 10:12/2  
Plan documents, 10:12/2  
Private right to sue, 10:9/3, 10:11/5

Psychotherapy notes, 10:12/2  
Security, 10:1/3, 10:3/7, 10:5/3, 10:9/4, 10:10/3, 10:11/6, 10:12/5  
“Standard of care,” HIPAA as, 10:9/3, 10:11/5  
State privacy laws, 10:7/6  
Transactions and code sets, 10:1/8, 10:3/3, 10:4/7, 10:7/4,  
10:12/6  
Wellness programs, 10:4/6, 10:5/2, 10:11/4

### Index of Cases

*Baum v. Keystone Mercy Health Plan*, 10:11/5  
*Bingham v. Allina Health System*, 10:2/7  
*Brown v. Mortensen*, 10:7/6  
*Cleveland Clinic Found. v. U.S.*, 10:4/4  
*Cooney v. Chicago Pub. Schs.*, 10:2/3  
*E.L. v. Scottsdale Healthcare Corp. Health Plan*, 10:6/7  
*IMS Health Inc. v. Sorrell*, 10:1/2, 10:1/5, 10:6/2, 10:7/8  
*I.S. v. Washington Univ.*, 10:9/3  
*Miguel M. v. Barron*, 10:6/6  
*Monarch Fire Protection Dist. v. Freedom Consulting &  
Auditing Servs., Inc.*, 10:9/2  
*Ortega v. Colo. Permanente Group, P.C.*, 10:12/3  
*Pacosa v. Kaiser Found. Health Plan of the Northwest*, 10:2/5  
*Pressley v. CaroMont Health Inc.*, 10:5/4  
*Quintana v. Lightner*, 10:4/3  
*Seff v. Broward County*, 10:5/2

### Special Offer for Thompson Subscribers

Receive a **\$25 DISCOUNT** on your  
next online purchase when you  
register with Thompson.com


As a registered user, you can

- Access your online products and tools
- Search your newsletter archives
- Manage your account information
- Renew your subscription(s)
- Receive news updates
- Take advantage of subscriber-only offers

Register today to create your online account. If  
you've already registered, we invite you to review  
and update your account. We'll give you **\$25 off**  
your next online purchase.

Visit [www.thompson.com](http://www.thompson.com), click on the Login icon and use the Web Offer Code 120182\* on your next  
online purchase to receive your \$25 discount.

\*This offer is valid on future purchases only. Cannot be used with other special offers or used as payment for prior purchases or renewals.

 THOMPSON