

# HIT News

*Emerging and Secondary Uses of Health Information Affinity Group Spotlight*

## Emerging and Secondary Uses of Health Information: An Overview of Uses and Legal Issues

**Daniel H. Orenstein, Esquire**  
*athenahealth, Inc.*  
Watertown, MA

**Stephen W. Bernstein, Esquire**  
*McDermott Will & Emery LLP*  
Boston, MA

**Linda S. Ross, Esquire**  
*Honigman Miller Schwartz & Cohn LLP*  
Detroit, MI

### I. Introduction

Beyond “treatment, payment and operations,” health information increasingly is being created, distributed, and used in many new ways. Some of these uses of health information have been around for some time and now are becoming more widespread, such as use in quality and outcomes measurement and clinical research. Others have emerged only recently, such as healthcare peer-to-peer networking and the use of personal health records. This article identifies a number of these “emerging and secondary uses” of health information as well as some of the potential legal issues associated with them.

This article does not attempt to identify every emerging and secondary use of health information. Instead, it focuses on some of the more prevalent uses and also examines a number of key legal issues associated with these uses. Another taxonomy of emerging and secondary uses that is worth consulting is “Secondary Uses and Re-uses of Healthcare Data: Taxonomy for Policy Formulation and Planning,” published by the American Medical Informatics Association.<sup>1</sup>



## Table of Contents

Emerging and Secondary Uses of Health Information: An Overview of Uses and Legal Issues <i>Daniel Orenstein, Esq., Stephen Bernstein, Esq., and Linda Ross, Esq.</i> .....	1
Editor’s Corner <i>Rebecca Williams, RN, JD</i> .....	11
The CMS Value-Based Purchasing Transformation: Starting on the Edges and Moving In <i>Gerald Tracy JD, MPH</i> .....	12
Chair’s Corner <i>Edward Shay, Esq.</i> .....	19
Staying Safe in the Internet’s Wild Wild West <i>Patricia King, Esq.</i> .....	20



*HIT News* © 2008 is published by the American Health Lawyers Association. All rights reserved. No part of this publication may be reproduced in any form except by prior written permission from the publisher. Printed in the United States of America. “This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.”  
—from a declaration of the American Bar Association



Many of the legal issues are familiar, such as compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security standards, but they may in some cases present unsettled concerns or require novel applications. Others, such as permissible uses of consumer-generated health content under private website terms and conditions of use, are new legal concerns that typically do not arise in a traditional healthcare context. This article does not attempt to draw conclusions on these issues; rather, it seeks to raise them for awareness and further exploration by members of the Health Information and Technology (HIT) Practice Group.

## II. Healthcare Social Networking

### A. Description of Use

Traffic on social networking websites where users can share information on specific medical conditions, such as TauMed.com, WegoHealth.com, Healingwell.com, and PatientsLikeMe.com, has increased significantly. These websites use forums, chat rooms, newsletters, user queries, and other methods of information exchange to facilitate sharing of experiences, advice, support, and knowledge on various health conditions. Peer-to-peer interaction,

rather than expert opinions and guidance, are the focus of these online websites.

What is unique about these social networking sites is that the information shared is primarily user-created (i.e., patient-created) content and often is individually identifiable. Typically, no covered entity is involved in the cycle of use, creation, and disclosure of the health information. The website host usually is not a covered entity, and the users offer the content on their own without a provider, payor, or other third party acting as an intermediary. Ultimately, research organizations, payors, providers, and others might be end users of data generated by the websites.

### B. Legal Issues

When individual users share information about a health condition, personal identifying information usually is required. This means that the information provided is personally identifiable health information; however, it might not be protected health information (PHI) as defined under the HIPAA privacy standards (the Privacy Rule) because it is not “created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse.”<sup>2</sup> The use and disclosure of this health information is subject to the terms and conditions of use agreed upon between the user and the host of the social networking website. In some cases, these terms and conditions simply promise standard confidentiality protections. In others, a good deal of thought has gone into the terms and conditions of use, including the right to disclose aggregated information to end users. In other cases, if the health information includes information obtained from or linked to a medical record, there may be third party end users, such as payors or providers, raising the issue of whether the information is PHI subject to the Privacy Rule.

Another issue to consider is whether certain uses contemplated by the website host are permitted by the terms and conditions of use, for instance, using discussions or demographic information posted on the site for marketing or to provide data on the perceived outcomes of a particular therapy. Even if certain uses are permitted by the website terms and conditions of use, there may be state laws that prohibit certain uses and disclosures of the health information. Website hosts walk a fine line when attempting to offer functionality that supports the exchange of medical information, medical opinions, and judgments, which activities could be construed as offering clinical advice. Usually, the terms and conditions of use for the sites typically provide that the information found on the site is for informational or educational purposes only, is not medical diagnosis or treatment advice, and should not substitute for the advice of a medical professional.

Another issue that promises to be contentious is the ownership of the health data on the site. Although the terms of use might grant various rights to the site host to use and disclose information submitted to the site, there may be competing claims on the ownership of the information. For example, if the terms and conditions

of use grant ownership to the site host, those terms may be at odds with a state law that gives a patient ownership of his or her health information.

### III. Personal Health Records

#### A. Description of Use

While definitions of personal health records (PHRs) vary, PHRs essentially offer a means by which individuals can store and access some or all of their health information for their own use and health management. A PHR can be in any form; however, in recent years, the development and availability of electronic PHRs has expanded rapidly. These offer an electronic means, ideally in a confidential and secure environment, by which individuals can access, maintain, manage, and share their health information, including personal information that can be entered into the record by the individual and/or by physicians, labs, and other healthcare providers or organizations.

Like electronic health records, PHRs are touted for their potential to improve healthcare, reduce costs, and confer on individuals a means by which they can better coordinate their own care. Employers, hospitals, and health plans are among those offering PHRs. PHRs also have become increasingly available to consumers over the Internet by companies such as WebMD, Google, Microsoft, and other consumer-focused companies.

PHRs vary in sophistication from a simple repository of information to an integrated tool enabling the individual to manage a medical condition. The notion of establishing a networked environment enabling individuals to establish secure connections with multiple entities that maintain PHI about them or their families has been endorsed by the Markle Foundation in its publication, "Connecting Americans to Their Healthcare: A Common Framework for Networked Personal Health Information,"<sup>3</sup> as beneficial not only to individuals but to healthcare entities as well. Such a networked environment potentially would enable a consumer to download copies of his or her medical history, review and update a medication history and allergies list, check immunization records, and review post-operative instructions, among other functions. Not surprisingly, vendors have established various programs providing interfaces between electronic health records (EHRs) and PHRs enabling information recorded in the EHR to flow through to the PHR. The potential use of PHRs on a more interactive basis by others has drawn attention in the wake of disasters such as Hurricane Katrina due to the need to enable patients to access their health information during a crisis.

#### B. Legal Issues

The principal legal concerns about PHRs are patient privacy, security, and integrity of the information stored or made accessible by the PHR. While HIPAA offers some protection, those protections can be viewed as limited and even inadequate because



many secondary users of PHI simply are not subject to HIPAA. Likewise, state privacy laws may not address the evolving uses of PHI. The lack of adequate privacy and security creates concerns that PHRs may be subject to security breaches and unauthorized acquisition of PHI stored on them.

Among other legal issues to consider are:

1. Who may appropriately own or control access to and use of, information contained in a PHR and under what circumstances? How should access to the PHR be managed and who decides, for example, what type of user authentication will be required to access a PHR? The answers to these and other concerns may vary based on a number of factors, such as whether the source of the information in the PHR is the individual or a provider, or both, and whether the PHR is provided by an employer, a health plan, or is created by the patient from an Internet site.
2. Under what circumstances will an individual be deemed to have authorized or consented to access or use of information housed in a PHR?
3. How can the accuracy and reliability of the information in a PHR be protected? Accuracy can be of concern depending on how the information included in a PHR is created and updated. Inaccurate and stale information may give rise to professional liability claims. The potential for such claims are of natural concern to physicians and other healthcare providers. What is their duty to provide, transfer, or update information into a patient's PHR or to rely on information included in a patient PHR?

Appropriate terms and conditions of use should be established to address these and other issues. Although guidelines for best practices for the use of PHRs are developing, the lack of widely adopted uniform standards and policies for such use makes it difficult, at this time, to point to an industry standard by which such use should be judged.



### IV. Consumer-Directed Financial Management Websites

#### A. Description of Use

Consumer-directed healthcare typically refers to programs, plans, and efforts by employers, payors, and other purchasers of healthcare to increase involvement of consumers in making healthcare decisions and choices. These “hands-on” initiatives are attracting attention as a means of controlling healthcare costs and enhancing quality by giving consumers greater financial control and decision-making authority over their healthcare. Consumer-directed healthcare initiatives commonly have some type of a health fund or savings account (such as a health reimbursement account, medical savings account, health savings account, or flexible spending account), a high deductible and co-payments for medical coverage (other than for preventive care), and online tools to facilitate smart healthcare decision-making by consumers. Typically, these programs set aside funds for medical expenses to be managed by consumers and seek to incentivize consumers to become more knowledgeable, responsible, and efficient in their use of healthcare services without sacrificing quality. This movement of consumers assuming personal and financial responsibility for their own care should only continue to grow.

Information technology is an essential component of a consumer-directed healthcare program. For example, health plans are expanding their technology offerings beyond the management of claims to more widespread management of health and benefits by employees. Product offerings for such items as healthcare, dental care, long term care, and pharmacy coverage are being coupled with online health assessment and prevention tools intended to enhance consumer healthcare decision-making and promote smarter decision-making by consumers. Such tools enable consumers to evaluate health risks and symptoms and to discern when immediate medical attention is needed. Many such programs are managed by consumers online and require the transmittal of personal health and financial information to a

sponsoring site where that information is processed and managed by the sponsor. Users access the site through user identification and passwords and can access links to information about cost and quality of healthcare providers and services as well as links to review past expenditures, project future needs, and to otherwise manage their financial accounts.

It is not unusual for a company, such as a bank, to partner with an information technology company to create platforms enabling health plans, employers, and third party administrators to administer consumer-directed healthcare accounts. The programs may offer “full service” by way of features such as financial claims adjudication, account management, a single sign-on portal to access account management and tools, investment options, and a payment card that automatically deducts amounts for selections made by consumers, among other services.

#### B. Legal Issues

Legal issues associated with consumer-directed healthcare programs also principally involve concerns about privacy and security of PHI and other financial information. Information housed on the site on which consumers direct their care and financing of that care may be accessed and used not only by the consumer but also by employers, plans, other payors, banks, or others involved in administering parts of the program. The risk of a breach of confidentiality is greater given the expanded access to such information. It is important to identify exactly who will use and access the information; under what circumstances; and which laws apply to such access, use, and disclosure. Although some of those accessing the information are subject to HIPAA, some (e.g., banks administering payment accounts) are not. Other legal concerns include the potential for misappropriation of information; identity theft and fraud; and proper authorization or consent to the access, use, and disclosure of the information.

### V. Pay for Performance, Quality Reporting, and Outcomes Measurement

#### A. Description of Use

Governmental and private payors as well as consumers have begun to demand performance as a basis for reimbursement of healthcare providers, creating a demand for patient information, both individually and in the aggregate, that is readily available, accurate, and tracks the outcomes of particular treatments. Sometimes referred to as “pay-for-performance” or “P4P” which also is discussed in another article of this issue of *HIT News*, this concept is taking hold and is showing some promise as a basis for payment that can promote best practices.

Accurately measuring health outcomes is difficult in many respects, including proving that a particular treatment protocol caused a particular clinical outcome. As a result, many P4P methodologies currently embrace an “activity” tracking methodology that measures whether certain tests and other actions were performed at certain intervals. For example a P4P program

might track whether a diabetes patient's HbA1C test was taken regularly, or whether regular cholesterol and blood pressure screenings were performed and corresponding prescriptions of statins and other medicines were prescribed. An alternative, and arguably more useful methodology, involves measuring indicia of a patient's health over time (such as the absence of sick-visits or hospitalizations), not simply activity or compliance with treatment protocols.

A recent example of this methodology is Medicare's Home Health Pay for Performance Demonstration program in which an incentive pool will be funded from savings accrued from the reduction in the use of more costly Medicare services. The pool will be shared by home health agencies that produce the highest level of patient care based on the following seven measures: incidence of acute care hospitalization, incidence of emergent care, improvement in bathing, improvement in ambulation, improvement in transferring, improvement in management of oral medications, and improvement of status of surgical wounds. Seventy-five percent of the incentive pool will be shared with those agencies in the top 20% of the highest level of patient care; 25% of the pool will be shared with the top 20% of those making the biggest improvements in patient care. If there are no savings, there will be no incentives.

Measuring and evaluating various health indicators not only will require more sophisticated data categories, but also better methods to capture data about specific patients as they move through the healthcare system among different providers, while at the same time identifying methods of attributing outcomes to particular care protocols. In its December 21, 2007, report to the Department of Health and Human Services, the National Committee on Vital and Health Statistics noted that reaching this kind of reporting ideal can be challenging because it "require[s] more clinical rich information than what is available solely from claims data."<sup>4</sup> In other words, methodologies for capturing this kind of information remain imperfect.

## B. Legal Issues

Although many of the challenges that payors face in obtaining information to implement P4P is technological, e.g., the technology simply is not sophisticated enough or available to clinicians, there are legal barriers as well, real or perceived. Due to privacy concerns, some providers are reluctant to voluntarily provide health information to payors. While HIPAA permits a physician to share a patient's health information with the patient's health plan for certain purposes, some physicians believe that health plans request too much information in a manner that conflicts with the physicians' contract with the plan.

A legal issue also arises with respect to remote access of EHRs. Some health plans have offered to provide case nurse reviewers to review patient paper records or in instances where a provider does maintain an EHR, remote access to the health plan's case nurse reviewers. Remote access presents privacy and security concerns, including whether the provider has satisfied HIPAA's minimum-necessary standard.

Among other issues are:

1. Once the information is obtained, if used by the acquiring health plan to generalize about particular populations and such conclusions are drawn from the collation of PHI, has the participating physician and the recipient health plan engaged in research without patient authorization in violation of HIPAA?
2. What should patients be told about data gathered about them, or should they be left to assume that the information is being gathered ultimately for their benefit, both in terms of quality and cost-effectiveness of care and pursuant to their agreement with their health plan?
3. What rights, if any, should physicians have with respect to publication of their own performance statistics? This last issue has gained prominence because at least three states in the past year (New Hampshire, Maine, and Vermont) passed legislation to limit or prohibit access to prescribing data without *physician* consent. Each of these statutes, however, has been the subject of intense litigation and, in at least two cases, has been struck down as unconstitutional (but remain subject to appeal).<sup>5</sup>



P4P is here to stay as a concept, but it appears to have a long way to go from a logistical, technological, and legal standpoint.

### VI. Payor Access to Electronic Health Records

#### A. Description of Use

In addition to more typical uses of health information by payors for quality and utilization management, payors have become interested in tapping into the growing availability of health information available through EHR systems. The EHR systems might be part of a regional health information exchange (or other health information exchange), or part of the information system of an academic medical center. The payor knows that it is technically possible to access the health information for purposes of (i) determining appropriateness of medical payments; (ii) evaluating treatment patterns; (iii) monitoring quality of treatment protocols and other potential uses; and (iv) to detect fraud and abuse.

While payors historically have had access to patient medical records to determine medical necessity and for auditing purposes, there is an increased push by payors for access to EHRs on a broader scale at any time for the above purposes. It is the quantity of available information along with the unprecedented levels of access to health records that raises new legal concerns.

#### B. Legal Issues

Among the key legal concerns raised are:

1. On what basis does a payor have the right to access and use health information of a provider and patients in an EHR system? The requested uses and disclosures should be reviewed carefully to determine whether they are permitted under the treatment, payment, and healthcare operations provisions of the Privacy Rule. Also, depending on the scope of uses or disclosures, the access by payors may need to be disclosed to patients in the provider's Notice of Privacy Practices;
2. Whether the scope of use of the information is permitted under the terms and conditions of use of the relevant EHR system or health information exchange through which the payor obtains the information;
3. If the information accessed is de-identified, then scope of access is not an issue, provided that the information was properly de-identified. If the information is a limited data set, then the use must be permissible (e.g., healthcare operations) and comply with the terms of the data use agreement.

### VII. Clinical And Database Research

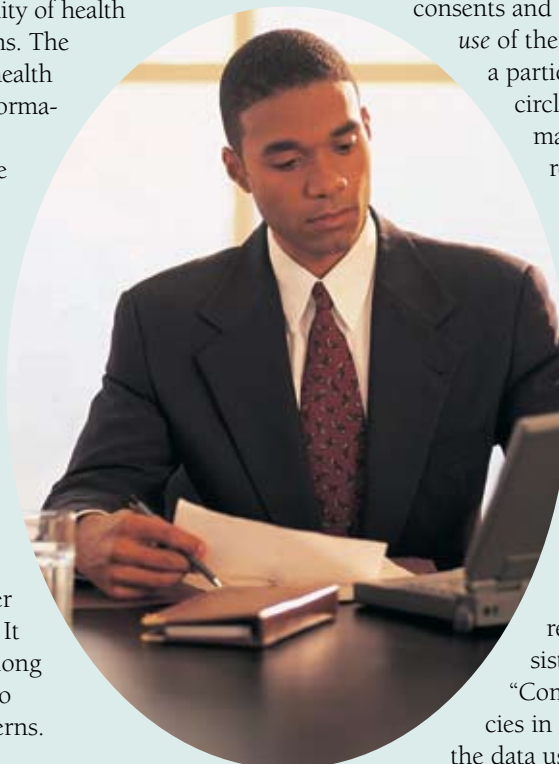
#### A. Description of Use

The increasing availability of electronic databases and powerful computing tools that can perform queries and analyses across multiple databases is generating a new level of complexity in the field of clinical research. In the case of prospective clinical research, patients typically are required to sign informed consents and HIPAA authorizations that permit the use of their identifiable clinical information for a particular research project within a limited circle of parties to whom such information may be *disclosed*, e.g., researchers, sponsors, regulatory bodies, and subcontractors such as contract research organizations engaged by sponsors, statisticians, and others hired to facilitate the conduct of research. In the case of retrospective clinical research, records created for clinical purposes are collected, but then reviewed *retrospectively* through electronic queries, with the aim of identifying information components correlated to improvements in care.

#### B. Legal Issues

The most salient legal issue in the research context arises from the inconsistency between HIPAA and the so-called "Common Rule," specifically inconsistencies in the level of detail required to describe the data use to a subject/patient. For instance, it may be sufficient under the Common Rule to obtain a patient's consent to use the data for "cancer research." HIPAA, arguably, may require more specificity, such as that the use is for "pancreatic cancer research." Similar scope of informed consent/authorization issues arise in other contexts, such as: (i) if some of the data is moved into a limited data set, which is in turn used for yet another form of research such as cardiac research; (ii) another researcher uses additional databases to cross-match and correlate the data, or to identify research subjects; (iii) stored pancreatic tissue, without identifiers, is used for different and later research, such as cardiac research; and (iv) data stored in an electronic health record for treatment purposes is later used for research purposes.

Organizations confronting these issues must determine, among other things, whether it is better to obtain a waiver of HIPAA authorization and informed consent from an Institutional Review Board for these secondary uses, or instead to de-identify the data or create a limited data set and then use only those resulting data sets to conduct the research. A detailed analysis of the context and scope of potential uses must be performed to determine the best approach on these and other issues that may arise.



## VIII. Public Health Reporting

### A. Description of Use

From the very first public health study in which cholera was traced to a town's water well, the analysis of aggregated population data has been at the core of many public health activities. Especially in view of today's threats of bioterrorism, a critical public health function is to quickly identify clinical trends across multiple providers, to determine whether there is a threat to the larger population, and to identify the source of the health hazard.

Although available technology is at the level to effectively execute these data searches, it has been only with concerted and coordinated efforts by third parties, health information exchange or health departments, for example, working with clinical laboratories, that the effort to streamline this approach has begun to occur. In a recent example, an outbreak of measles in the Boston area quickly was traced to those working in a particular office building, but only after data became available through medical detective work and the sharing of data through a common clearinghouse, in this case the Massachusetts Department of Public Health. If providers do not report timely or departments of public health do not receive diagnosis reports quickly, then the speed at which these outbreaks can be identified is significantly compromised. With powerful computing tools and the widespread use of EHRs containing structured data (which allow, for example, meningitis to be coded the same way by every clinical laboratory), there is at least the theoretical possibility that an outbreak of meningitis could be identified quickly and the relevant organizations alerted.

### B. Legal Issues

HIPAA permits the reporting of health information to public health authorities. Similarly, most state laws address, and sometimes mandate, the reporting by healthcare providers of certain communicable diseases to state and/or local departments of health. Unfortunately, the number and complexity of these reporting laws make it difficult for the average physician to know his or her reporting duties. Further, the laws often are vague about whether conditions *must* be reported or simply *may* be reported. Due to privacy concerns, physicians increasingly are wary about whether a report must identify the patient by name.

For example, providing patient identifiable data can be a condition to federal funding of certain state HIV-prevention programs. The simple logistics of gathering the data presents legal issues for providers if they fail to report certain conditions as required by state law. As more providers implement EHRs and begin to enter into health information exchanges, there is the greater possibility of streamlining these reporting efforts by tagging reportable conditions such that they are *automatically* reported from a provider's EHR to the applicable department of health. Nevertheless, concern on the part of providers as to whether there might be "false-positive" reports,

i.e., reporting certain conditions that when viewed in context by the clinician (as opposed to a computer) should not have been reported, also presents legal concerns. To address these concerns, some health information exchanges are beginning to experiment with engaging a neutral third party clinician able to determine from coded, but de-identified, data whether a condition is reportable, and then flagging for the attending physician's review the case so the physician can determine affirmatively the need and the appropriateness of reporting such information to the department of health.

There is no doubt that the power of aggregating data across populations is key to fine-tuning the tracking of public health events and, in turn, improving public health. Although these efforts are beginning to take hold, there remains a strong need to educate both the public and the healthcare provider community about the technology involved and the corresponding legal pathways that currently exist—or that need to be created—to ensure that these efforts succeed.

## IX. Marketing

### A. Description of Use

PHI has significant value as a marketing tool because it enables hospitals, health plans, and other businesses to better tailor marketing initiatives to their target audiences. On the positive side, such information can be used by pharmacies to remind patients to refill their prescriptions for medication. It also can enable businesses to offer coupons or promote specific treatment, equipment, products, or regimens to individuals with certain health conditions or risks. Disease-specific information also can be disseminated more strategically through the use of PHI. The proliferation of PHI online provides broader access to those engaged in marketing initiatives. For example, marketing companies may monitor social/medical networking websites focused on a particular condition to assemble a targeted marketing list for a particular product.

On the negative side, businesses could seek to purchase, sell, and exploit PHI for less altruistic (i.e., commercial) purposes. Collecting PHI-related information based on consumers' Internet activity is a growing field for marketing firms and is called "behavioral tracking" or "behavioral targeting." In this process, an ever-evolving profile of individuals is created based on the web searches they run and the websites they visit. Based on this information, advertisements are targeted to particular individuals.

### B. Legal Issues

As more and more personal information becomes available on the Internet, the question becomes who may properly access, use, disclose, and even exploit the information. Are there or should there be disclosure statements or terms and conditions of use on the site agreed to by users? Who enforces violations of those conditions and at whose expense? Is there or should there be an overall data steward? What is a reasonable expectation of privacy

and security under these circumstances? Again, HIPAA offers some protection with respect to marketing but only with respect to uses and disclosures by covered entities and business associates. For example, to the extent that HIPAA applies, it requires covered entities to obtain patient authorization to use PHI for marketing purposes, with some exceptions.

If HIPAA does not apply, then PHI could be exploited in ways that may have other legal ramifications, especially in the consumer protection arena. In 2006, the Federal Trade Commission held public hearings to examine the emerging consumer protection issues arising due to technological advances. Behavioral tracking received significant attention in the hearings. The hearings and subsequent discussions on the topic highlighted potential legal concerns regarding a lack of transparency, damage to consumer autonomy, and information falling into the wrong hands or being used for unintended purposes.

Also, some companies have faced lawsuits for their attempts to track the Internet activity of their consumers. In 2002, a class action suit was brought against a marketing firm along with numerous other pharmaceutical companies. The marketing firm engaged in behavioral tracking, using software that gathered information submitted by consumers and that tracked their activities at the sites. The plaintiffs alleged violations under the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. Although defendants in that case won on summary judgment,<sup>6</sup> future cases with different facts could subject such companies to liability for tracking consumer health information.

Other potential legal concerns arising in the context of the purchase and sale of PHI include exposure under the federal Anti-kickback Statute and the Stark Law (as well as state counterparts).

## X. Business Analytics

### A. Description of Use

Many organizations in the healthcare industry have begun to use health information to better understand their business and organization. Organizations have been analyzing patient data, transaction data, service delivery data, and benchmarking, for example, to improve service, to control costs, and for risk management and strategic planning. These uses have expanded from the more common uses of health information for quality and utilization management. Organizations are establishing systems to monitor key performance indicators for their businesses. They have been drawing on internal resources to perform these analyses, as well as engaging external consultants.

### B. Legal Issues

Health information involved in business analytics might involve the use of limited data sets, de-identified information, or aggregated PHI. Some key legal issues to consider include:

1. If PHI is used, then the use or disclosure should be permitted by the Privacy Rule and/or the terms of a business associate contract. Many of the uses by a covered entity will be permitted as “healthcare operations.” If, however, the permitted use of “healthcare operations” (or another Privacy Rule permitted use) is not available, then patient authorization might be required. Use of PHI by a business associate for its “proper management and administration” may cover many of these uses.
2. If the data that is used is de-identified, then the organization must ensure that the data is properly de-identified in accordance with the methods set forth in the Privacy Rule and cannot easily be re-identified (matched back up with individually identifiable information).
3. If the data that is used is a limited data set, then the parties must ensure that the data is a proper limited data set, and used only for the purposes and in the manner permitted by the Privacy Rule and subject to a data use agreement. The Privacy Rule and any contractual provisions should be reviewed carefully to ensure that the use is in fact permitted.

## XI. Conclusion

Many of the trends described in this article represent subsets of overall societal and economic trends—for example peer-to-peer networking, enhanced consumer control, and accountability and critical analysis of more widely available data—and signs indicate that they will become important and powerful trends in the healthcare industry as well. The area of emerging and secondary uses of health information is dynamic and evolving, and the issues described above represent only a snapshot in time. These new uses of health information, and variations on existing uses, will continually challenge the legal framework within which they occur, promising much stimulating legal thinking and work in building and advising on appropriate legal pathways and models.

1 See [www.hhs.gov/healthit/documents/m20071113/07b-amia.pdf](http://www.hhs.gov/healthit/documents/m20071113/07b-amia.pdf).

2 See 45 C.F.R. § 160.103, definition of “individually identifiable health information.”

3 See [http://connectingforhealth.org/commonframework/docs/P9\\_NetworkedPHRs.pdf](http://connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf).

4 See [www.ncvhs.hhs.gov/0712211t.pdf](http://www.ncvhs.hhs.gov/0712211t.pdf).

5 See *IMS Health Incorporated et al. v. Sorrell*, No. 07-188, (D. Vt., filed 8/29/07), Defendants’ Consented-to Motion for Extension of Time to Respond to Phrma’s Motion for Partial Summary Judgment, 4/4/08; *IMS Health Incorporated; Verispan, LLC; Source Healthcare Analytics, Inc. v. G. Steven Rowe*, United States Court of Appeals for the First Circuit, No. 08-1248, (filed 3/4/08), Order entered by Judge Sandra L. Lynch, the consent motion to stay appellate proceedings is granted until *IMS Health, Inc. v. Ayotte*, No. 07-1945, is decided, 3/24/08; *IMS Health Incorporated; Verispan, LLC v. Kelly A. Ayotte*, United States Court of Appeals for the First Circuit, No. 07-1945, (filed 6/20/07), Case argued, 1/9/08.

6 See *In re Pharmatrak, Inc. Privacy Litig.*, 220 F. Supp. 2d 4 (D. Mass 2002); 329 F.3d 9 (1st Cir 2003); 292 F. Supp. 2d 263 (D. Mass 2003).

**Copyright 2008 American Health Lawyers Association, Washington, D.C.**

**Reprint permission granted.**

**Further reprint requests should be directed to**

**American Health Lawyers Association  
1025 Connecticut Avenue, NW, Suite 600  
Washington, DC 20036  
(202) 833-1100**

**For more information on Health Lawyers content, visit us at [www.healthlawyers.org](http://www.healthlawyers.org)**