Chapter 5

Commerce In Provider Data: What, Why And Provider Contractual Controls

By Daniel F. Shay

KeyCite®: Cases and other legal materials listed in KeyCite Scope can be researched through the KeyCite service on Westlaw®. Use KeyCite to check citations for form, parallel references, prior and later history, and comprehensive citator information, including citations to other decisions and secondary materials.

§ 5:1 Introduction—Why does data matter?

On April 27, 2004, President George W. Bush signed Executive Order 13335, establishing a new healthcare policy to develop "a nationwide interoperable health information technology infrastructure," and creating the position of National Health Information Technology Coordinator.[1] As part of the agenda, the new infrastructure should "[promote] a more effective marketplace, greater competition, and increased choice through the wider availability of accurate information on healthcare costs, quality, and outcomes."[2] On July 21, 2004, then-recently appointed National Coordinator David J. Brailer, M.D., Ph.D. published a Framework for Strategic Action in implementing the President's order.[3] The report details several general steps to achieve the President's goal, including enhancing informed consumer choice, and streamlining quality and health status monitoring. In calling for enhanced consumer choice, the report states "Consumers should be informed about clinicians and institutions based on what the consumer values, including, but not limited to, the quality of care that the provider has historically delivered."[4] With respect to health status monitoring, the report advocates using de-identified individual health care data to "detect and address quality variations, to enable consumer choice, and for many other functions . . . . A streamlined quality monitoring infrastructure will allow for

---

[Section 5:1]

[1]Executive Order 13335, 69 Fed. Reg. 24059 (Apr. 27, 2004).

[2]Executive Order 13335, 69 Fed. Reg. 24059 (Apr. 27, 2004).

[3]Brailer, "The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care—Framework for Strategic Action" (July 21, 2004), available at http://www.os.dhhs.gov/healthit/.

[4]Brailer, "The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care—Framework for Strategic Action," 22 (July 21, 2004), available at http://www.os.dhhs.gov/healthit/.

a complete look at quality and other issues in real-time and at the point of care, while also minimizing intrusions and burdens imposed on clinicians."[5] These two quotes illustrate one side of an underlying tension in the healthcare industry today: the desire for greater transparency in healthcare through publication of data—and ideally the improvement of quality resulting from such publication. But the increased policy value on transparency is juxtaposed against providers' often expressed concern for privacy and confidentiality of such data.[6]

The drive for transparency has received considerably increasing policy support. In 2001, the Institute of Medicine ("IOM") published *Crossing the Quality Chasm*, outlining key problems in healthcare quality and providing recommendations for how to improve performance.[7] Among the recommendations, the IOM advocated

> for health systems to be accountable to the public; to do their work openly; to make their results known to the public and professionals alike; and to build trust through disclosure, even of the systems' own problems. . . . In the future health care system, the rule should be: *Have no secrets. Make all information flow freely so that anyone involved in the system, including patients and families, can make the most informed choices and know at any time whatever facts may be relevant to a patient's decision making*.[8]

On the other side of the debate, however, lie the legitimate concerns of the providers. Providers may question the accuracy of reporting. Does the report accurately portray the provider, and if not, what provider challenges can be mounted? Is the report fair? Does the report utilize measures of actions within the provider's control, or does it track

---

[5]Brailer, "The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care—Framework for Strategic Action," 25 (July 21, 2004), available at http://www.os.dhhs.gov/healthit/.

[6]Although, there is some dispute as to how effective methods such as report cards are at engendering quality improvement. *See* Gosfield, "The Performance Measures Ball: Too Many Tunes, Too Many Dancers?," *Health Law Handbook*, 31 (A. Gosfield, ed. 2005).

[7]Corrigan et al., eds., Crossing the Quality Chasm (National Academy Press, Wash. D.C., 2001).

[8]Corrigan et al., eds., Crossing the Quality Chasm 79-80 (National Academy Press, Washington, D.C., 2001).

aspects of performance that are unaffected by the provider's behavior? Most importantly, providers will naturally fear the use of such reports against them in litigation, even if the provider generally supports the notion of transparency to enhance quality.

In addition, as the healthcare industry warms to the idea of increased transparency and freedom of access to provider data, the commercial value of provider data will increase. Thus, providers may recognize the potential benefits of trading data, as well as their need to control such data. Providers now have an economic interest in controlling data that extends beyond merely ensuring that they are not misrepresented publicly; a provider may now benefit from the sale or licensing of their data to a database or clearinghouse. It is therefore that much more important to pay close attention to contract language which may deprive a provider of control over its data.[9]

However, before discussing the value of or means of controlling such data, it is important to understand what type of data providers can and cannot control and particularly what data a provider "owns" and can therefore exercise dominion over in ordinary legal terms. Towards this end, a definition of "proprietary" information is important, especially as it relates to "private" or "public" information. In the following discussions, incidentally, the contractual language addressed comes from actual contracts.

§ 5:2 Introduction—Why does data matter?—Proprietary information

"Proprietary" information may take a number of forms. It may include materials subject to specific statutory protections, such as in trade secret, copyright, and patent law; or it may simply be material which is specifically created by the provider, but is afforded no statutory protection, such as customer lists, strategic or marketing plans, or other similar business relevant information. "Proprietary" information may be defined differently, depending either on the nature of the information itself, or on the mechanism by which it is defined. Often a contract will define "proprietary" information as broadly as possible, so as to grant the party who

[9]*See* § 5:3.

owns or creates the data the maximum protection and control of the information. As is typical in other business settings where control over data is sought, a major pharmaceutical company, in a form contract with prospective vendors defined "proprietary" information as:

> All information, whether written or oral with respect to the conduct or details of the businesses of [Company] and its Affiliates including, without limitation, any Proprietary Documents (hereinafter defined), methods of operation, procedures, facilities, formulae, customers and customer lists, compounds, products, proposed products, former products, prices, fees, costs, plans, designs, technology, inventions, trade secrets, know-how, software, marketing methods, policies, plans, personnel, suppliers, competitors, markets or other specialized information or proprietary matters of [Company] or any of its Affiliates.
>
> "Proprietary Documents" means all data, designs, drawings, blueprints, tracings, sketches, plans, layouts, specifications, models, programs, cards, tapes, disks, printouts, writings, manuals, guides, notes and any and all other memoranda, including without limitation any and all written information which may be or has been furnished to Vendor or which may be produced, prepared, or designed by Vendor in connection with its duties hereunder.

While much of the material addressed might well be protected under statutory law (such as any material subject to federal copyright or patent protection, or protected by state trade secret law), or even in the common law, the clauses above sought to maximize the scope of the definition and bind the other party to acknowledging the owner's control of the use of such information. For purposes of this chapter, "proprietary" information will be considered any information that is not generally a matter of public record, and over which the provider may seek to assert both control and ownership.

§ 5:3 Introduction—Why does data matter?—Private information

In contrast with "proprietary" information, "private" information is information which is not a matter of public record, but over which the provider cannot exercise exclusive control, or about which the provider cannot claim excusive ownership. In healthcare, the Health Insurance Portability and Account-

ability Act ("HIPAA")[1] offers the most obvious example of "private" information.

Under HIPAA, a patient's Protected Health Information ("PHI") is defined as "individually identifiable health information" which is transmitted by or maintained in an electronic medium or transmitted or maintained in any other form or medium.[2] Providers are required to maintain the information as confidential and are not permitted to disclose except under specific circumstances.[3] The information therefore cannot be considered in any way public.

However, providers are also subject to numerous additional requirements regarding PHI. For example, a provider must generally grant a patient access to the patient's PHI, upon request[4] give the patient an accounting of all disclosures of that patient's PHI for the previous six years,[5] and grant the patient the opportunity to amend the patient's PHI.[6] Although the regulations permit the provider to deny the patient's request under certain circumstances, the provider does not retain exclusive control over the PHI. Thus, while not public, the information cannot be said to be "proprietary" to the provider.

§ 5:4 Introduction—Why does data matter?—Public information

"Public" information, in contrast with both "proprietary" and "private" information, is often far less clearly defined. In general, "public" information is generally available information, such as names, addresses, or telephone numbers (although even these may be "private," as when they pertain to patients). In addition, a definition of "public" information may be inferred by reference to what is not clearly "proprietary" information.

For example, a confidentiality clause in a contract may

[Section 5:3]

[1]45 C.F.R. Parts 160 and 164.

[2]45 C.F.R. § 160.103.

[3]45 C.F.R. § 164.502(a). *See also* 45 C.F.R. §§ 164.504 to 164.514.

[4]45 C.F.R. § 164.524(a).

[5]45 C.F.R. § 164.526(a).

[6]45 C.F.R. § 164.528(a).

state that proprietary or confidential information does not include information "(i) that is a matter of public knowledge on the date of this Agreement or (ii) becomes a mater of public knowledge after the date of this Agreement." A contract may also exempt:

> (a) Information, including but not limited to names, addresses, affiliations, and phone numbers, that [are] publicly available by means other than wrongful disclosure or lawfully obtained from third parties without any confidentiality obligations;
>
> (b) Information which is required by law or by a government agency to be disclosed by a receiving party, provided that such receiving party will immediately notify the disclosing party of the requirements for such re-disclosure and reasonably cooperate in obtaining any protective order desired by the disclosing party with regard to such information;
>
> * * *
>
> (d) Information disclosed to a receiving party if the disclosing party gives written authorization for the information to be re-disclosed, published, disseminated, released or distributed by the receiving party to another person.

However, comparing what is protected to what is not, and classifying unprotected information as "public" may still not yield a clear definition in all contexts. A court may consider certain information to be the property of a party to the case, but still may not extend common law or statutory protections to such information. Trade secrets are one area in which a court may refuse to extend the protections of the law to information that it nonetheless considers the property of one of the parties.

In *In re Urgent Medical Care, Inc.*,[1] Urgent Medical Care, Inc. ("UMCI"), an occupational therapy practice, sued Bugay, its former marketing director for sharing their proprietary information with a third party in attempting to secure the third party as a new client of the director. While employed with UMCI, Bugay had access to client profiles and treatment practices, financial information, fee schedules, and the identity of employers who used UMCI's services for their

---

[Section 5:4]

[1]In re Urgent Medical Care, Inc., 153 B.R. 784 (Bankr. S.D. Ohio 1993).

employees.[2] During the course of his employment at UMCI, but unbeknownst to UMCI and purely for his own benefit, Bugay approached MedOhio, a physician practice run by Ohio State University, to provide management services for MedOhio's occupational health care program.[3] In the course of his negotiations with MedOhio, Bugay disclosed the proprietary information, to demonstrate the volume of business that Bugay claimed he serviced.[4] The court held that a list of customers, while the property of the plaintiffs, did not qualify for protection under Ohio's trade secret law. "Even though the Court finds that the employer client list belongs to UMCI, it does not automatically follow that the list is a trade secret within the definition of [Ohio's Trade Secret law]. . .. The identity of these employer clients is simply a list of much of the universe of business employers likely to need occupational health care services in Central Ohio."[5]

Similarly, in *Carriage Hill Health Care, Inc. v. Hayden*,[6] Carriage Hill, a dental supply company, maintained certain customer information which included customer names, addresses, telephone numbers, contact persons, histories, ratings, and potential for future purchases. When Hayden, a former employee of Carriage Hill, left to seek new employment, he used this information to contact Carriage Hill's customers.[7] Carriage Hill brought suit against him, asserting, among other claims, that he had violated New Hampshire's trade secrets act.[8] In discussing Carriage Hill's claim of misappropriation of trade secrets, the court noted that a mere list of customers' names, addresses, and telephone numbers could not be a trade secret, specifically because

---

[2]In re Urgent Medical Care, Inc., 153 B.R. 784, 786 (Bankr. S.D. Ohio 1993).

[3]In re Urgent Medical Care, Inc., 153 B.R. 784, 786 (Bankr. S.D. Ohio 1993).

[4]In re Urgent Medical Care, Inc., 153 B.R. 784, 789 (Bankr. S.D. Ohio 1993).

[5]In re Urgent Medical Care, Inc., 153 B.R. 784, 789 (Bankr. S.D. Ohio 1993).

[6]Carriage Hill Health Care, Inc. v. Hayden, 13 I.E.R. Cas. (BNA) 852, 1997 WL 833131, at *5 (D.N.H. 1997).

[7]Carriage Hill Health Care, Inc. v. Hayden, 13 I.E.R. Cas. (BNA) 852, 1997 WL 833131, at *1 (D.N.H. 1997).

[8]Carriage Hill Health Care, Inc. v. Hayden, 13 I.E.R. Cas. (BNA) 852, 1997 WL 833131, at *7 (D.N.H. 1997).

such information was "readily ascertainable" by examining a telephone directory for entities providing dental care.[9] However, information including ratings of a customer's potential for future purchases and a list of prices charged to the customers did qualify for trade secret protection, specifically because such information was not "readily ascertainable."[10] The court also found that there was sufficient evidence that Hayden had used this protected information in soliciting business, so his motion to dismiss could not be granted.[11]

In both of these cases, had contracts governed the relationships between the parties and specifically set forth their rights with respect to data, the courts would have been able to apply a wider scope of protection. If the court in *Bugay* had not been bound solely by trade secret law, it could have granted protection to the information that the contract stated was UMCI's property.

Given the far greater interest in healthcare data, which both originates with and is about providers, this chapter will discuss how hospitals and/or physicians (hereinafter referred to generally as "providers") may control and protect their data in contractual relationships with third parties, even when those relationships are not primarily about data. Providers may disclose data as part of a relationship about other activities, from a managed care participation agreement, to contracting with a management company to manage the practice, to a billing company contract, to a contract with a software vendor for an electronic medical record.[12] These relationships may place the provider at a disadvantage, if it loses control of valuable information. However, rather than focus exclusively on remedies in the courts, this

---

[9]Carriage Hill Health Care, Inc. v. Hayden, 13 I.E.R. Cas. (BNA) 852, 1997 WL 833131, at *8 (D.N.H. 1997).

[10]Carriage Hill Health Care, Inc. v. Hayden, 13 I.E.R. Cas. (BNA) 852, 1997 WL 833131 (D.N.H. 1997).

[11]Carriage Hill Health Care, Inc. v. Hayden, 13 I.E.R. Cas. (BNA) 852, 1997 WL 833131 (D.N.H. 1997).

[12]This chapter will not address many other relationships where the provider may provide or create data but will not have an explicit contractual relationship associated with the interaction, such as in the ordinary course of prescribing drugs and interacting with pharmacies, or as an independent medical staff member ordering hospital services for an inpatient.

chapter is primarily concerned with how to draft contracts with third parties, so as to best protect the provider's information.

§ 5:5 Third-Party Uses of Information

In considering how to protect a provider's information, it is essential to first understand how that information may be used. For example, a physician employed by a hospital will likely have his outcomes data monitored for submission to state health agencies. An HMO may republish data collected from physicians in advertising materials. Or, a hospital or HMO may sell data to a commercial database, which then further discloses the information. Depending on how the other party uses the data, a provider's disclosure of its information may result in the information losing its proprietary status and becoming a matter of public record. In most of the examples presented in this chapter, the information has become public. While this may not always be negative, providers should carefully consider how their data may be used by the party with which they contract, and whether and how that party will disclose the information to third parties.

§ 5:6 Third-party uses of information—Report cards

One of the primary mechanisms for gathering and distributing information relating to quality are the various health care report cards available to the public today. Usually, quality-oriented information is public information, but such public information is often compiled from information that could have been considered proprietary or private, prior to disclosure, and which is then aggregated and/or de-identified.

§ 5:7 Third-party uses of information—Report cards—State report cards

Within the state-mandated realm, states require submission of various information to be used in state report cards. Texas (Texas Health Care Information Council), Pennsylvania (Health Care Cost Containment Council), New Jersey (Department of Health and Social Services Division of Health Care Quality and Oversight HMO Performance Reports), Maryland (Maryland Health Care Commission Comprehensive Performance Report on Maryland HMOs and POS

Plans), and Indiana (State Department of Health Long Term Care Division Nursing Home Report Cards), as well as others, all have state report card systems or other quality tracking systems.[1]

Each of these report card entities has been empowered by the state legislature to collect provider data and publish it in report cards. Typically, the states collect information from hospital discharge data or claims data.[2] They may also collect HEDIS information or CAHPS data when reporting on HMOs.[3] Reports are usually presented to the public in either hard copies or on websites.[4] The reports themselves usually present information in bar graphs or with other graphical representations of quality, frequently using a "meets/exceeds/falls below state averages" indicator.[5] Measures presented vary considerably, depending on the report. They may only

---

[Section 5:7]

[1]V.T.C.A. §§ 108.001, et seq.; P.S. §§ 449.1, et seq.; N.J.S.A. 25:2S-15; N.J.A.C. 8:38A-4.16; Md. Code Ann., Health—General §§ 19-101, et seq.; COMAR 10.24.02.01, et seq.; IC 16-28-1-13; IC 16-19-3-25.

[2]"Your HMO Quality Checkup," Gulf Coast Texas Region, at 6; "Measuring the Quality of Pennsylvania's Commercial HMOs 2002," at 32; "Measuring the Quality of Maryland HMOs and POS Plans: 2004 Consumer Guide," at 3; "Comprehensive Performance Report: Commercial HMOs & Their POS Plans in Maryland," at 11 (Sept. 2004).

[3]"Where does THCIC data come from?," http://www.thcic.state.tx.us/IQIReport2002/IQIReportGuide.htm#DataSource; http://www.phc4.org/dept/dc/default.htm; New Jersey Hospital Report, 2004, Technical Report: Methodology, at 1; http://hospitalguide.mhcc.state.md.us/Misc/utilization_info.htm#analyses.

[4]*See generally* http://www.thcic.state.tx.us; http://www.phc4.org; http://hospitalguide.mhcc.state.md.us/index.asp; http://web.doh.state.nj.us/hpr/; http://www.state.in.us/isdh/regsvcs/ltc/repcard/rptcrd1.htm.

[5]"Your HMO Quality Checkup," Gulf Coast Texas Region, at 13, http://www.thcic.state.tx.us/Publications.htm; "Measuring the Quality of Pennsylvania's Commercial HMOs 2002," at 25, http://www.phc4.org/reports/mcpr/02/default.htm; "2004 New Jersey HMO Performance Report—Compare Your Choices," http://www.state.nj.us/health/hmo2004/; "Measuring the Quality of Maryland HMOs and POS Plans: 2004 Consumer Guide," at 6, http://www.mhcc.state.md.us/hmo/rptdesc2004.htm.

examine pneumonia and heart attack data, or they may include substantially more measures.[6]

By virtue of statutorily-created relationships between providers or health plans and the states, much of the disclosed information loses its proprietary nature and becomes public record. Once the information has become public, the provider will have very little ability to challenge the data in report cards. Even if the provider believes the measures or reporting methods used are unfair, the provider will often lack the ability to sue the responsible state agency because of its sovereign immunity. The provider will also lack the ability to prevent the further use of this data, even when such data is used against them at a trial for other reasons.[7]

§ 5:8 Third-party uses of information—Report cards—Private report cards

Unlike state report cards, private report cards are usually voluntary or use information that already is a matter of public record. In cases where the reporting is entirely voluntary, the party submitting data may be doing so in order to provide evidence of its own quality, or to obtain a financial benefit directly from the collecting entity. Some private report cards also track data that already has been made public.

The National Committee for Quality Assurance ("NCQA") provides both the Health Plan Employer Data and Information Set ("HEDIS®") and operates the Quality Compass® program. HEDIS® is compiled entirely from information voluntarily submitted by health plans, and tracks variables such as effectiveness of care, availability of and access to care, satisfaction with experience of care, cost of care, and use of services, among others. As evidenced above, HEDIS®

---

[6]*Compare* "Hospital Performance Report—Southeastern Pennsylvania" (Sept. 2004), http://www.phc4.org/reports/hpr/03/default.htm (using 29 different measures), *and* "New Jersey 2004 Hospital Performance Report," http://web.doh.state.nj.us/hpr/ (using only pneumonia and heart attack measures).

[7]Angelico v. Lehigh Valley Hosp., Inc., 984 F. Supp. 308, 313 (E.D. Pa. 1997), rev'd, 184 F.3d 268 (3d Cir. 1999) (court indicated that plaintiff's antitrust expert could have used PHC4 mortality and admission severity group data to offer opinion on quality of surgical care available in Lehigh Valley area in lawsuit claiming antitrust violations by hospital surrounding denial of privileges to plaintiff physician).

is widely used by plans and organizations preparing their own reports on quality. Quality Compass® is a program providing specific information on over 300 commercial HMO and point-of-service products. This publication derives information from HEDIS® data and presents it in a comparative format so that consumers may compare different plans based on the information collected. HEDIS® data is entirely voluntarily submitted by managed care organizations. Health plans often advertise their own HEDIS® results, as well as their accreditation or certification status by NCQA—a practice which NCQA encourages.[1]

HealthGrades.com offers report cards on physicians, hospitals, and nursing homes.[2] The physician reports offer such information as the physician's board certifications, disciplinary actions, education and training, and comparisons to national data. The physician reports draw data from a variety of sources, including state licensing boards; records of disciplinary actions; records indicating where a physician went to medical school; and where a physician performed internships, residencies, and fellowships.[3] For its hospital reports, HealthGrades.com gathers its information is primarily from two sources: CMS' MedPAR files, and discharge data required to be reported by hospitals in sixteen states.[4] For its nursing home reports, HealthGrades.com obtains its information from CMS' Online Survey Certification and Reporting database, CMS' Skilled Nursing Facility Complaint database, and from state resources.[5] Because the sources of information are mostly public records, providers

---

[Section 5:8]

[1]http://www.ncqa.org/Communications/Publications/NCQAUpdate/mar04update.htm#2.

[2]*See* http://www.healthgrades.com/consumer/index.cfm?TV__Eng=homepage.

[3]http://www.healthgrades.com/consumer/index.cfm?fuseaction=mod&modtype=FAQS&modact=FAQS&action=getOne&faq__id=37.

[4]http://www.healthgrades.com/consumer/index.cfm?fuseaction=mod&modtype=FAQS&modact=FAQS&action=getOne&faq__id=7.

[5]http://www.healthgrades.com/consumer/index.cfm?fuseaction=mod&modtype=FAQS&modact=FAQS&action=getOne&faq__id=37.

will be generally unable to challenge the reports, unless Healthgrades.com defames or misrepresents the provider.[6]

The Leapfrog Group, an independent organization made up primarily of employers who purchase healthcare services, allows consumers to search and compare hospital data in the consumer's geographic area.[7] Unlike HealthGrades.com, however, the Leapfrog Group collects its data from voluntarily submitted information, rather than from examining data that a state requires hospitals to report.[8] Generally, Leapfrog asks hospitals if they have implemented the four "quality and safety leaps" that Leapfrog has developed, which are: whether a hospital has implemented a computerized physician order entry system, whether a hospital meets certain minimum safety and volume requirements for performing specific procedures on high-risk patients, whether the hospital meets certain requirements for how its intensive care unit is staffed, and whether a hospital has put in place twenty-seven measures that Leapfrog has identified which reduce the potential for medical errors.[9] The information is presented to the consumer comparatively, so that the consumer may examine multiple hospitals within their area. In terms of the specific reports, hospitals are given a graphical indicator showing either that they: were not requested to respond to a given question, do not perform a given procedure, did not report, reported but have not met Leapfrog's standards yet, have shown a good early-stage effort in implementing the standards, have shown good progress in implementing the standards, or have fully implemented the standards.

The California Health Care Foundation ("CHCF") is a philanthropy group dedicated to the improvement of healthcare quality in California.[10] CHCF publishes an annual report: the California Health Care Market Report. "Most of the data are drawn from public sources, including the annual statements that HMOs must file with the California

---

[6]This chapter does not address issues regarding defamation or misrepresentation by reporting agencies.

[7]*See generally* http://www.leapfroggroup.org.

[8]http://www.leapfroggroupdata.org/cp.

[9]http://www.leapfroggroup.org/for__consumers/hospitals__asked__what.

[10]http://www.chcf.org/aboutchcf/.

Department of Managed Health Care and the annual surveys that hospitals submit to the Office of Statewide Health Planning and Development."[11] However, in certain instances, sources of information also included responses to survey questions completed by the HMOs themselves and submitted to the HMOs by the author of the report, as well as HEDIS® information from NCQA.[12] The report itself tracks a wide variety of information, including HMO enrollment, member satisfaction, HMO revenues and net income, capitation rates, and others.[13]

The New York State Health Accountability Foundation ("NYSHAF"), offers its own New York State HMO report cards.[14] The report cards use data sources from the New York State Department of Health, which requires HMOs to submit both HEDIS® data (including certain tailored issues specific to New York State—such as lead testing of two-year-olds), as well as consumer opinions.[15] Based on this information, the NYSHAF develops reports that allow consumers to compare a wide variety of data in two general categories: access and service, and staying healthy/getting better. These two categories are then broken into sub-categories, which include overall quality (based on member satisfaction), ability to get needed care, primary care physicians who are board certified, portions of pregnant women receiving early prenatal care, portion of members with high blood pressure that was under control, and other measures.

In all of the above examples, be they state-mandated, private and voluntary report cards, or private pay-for-performance initiatives, the reporting: (1) drew upon information that was often a matter of public record; (2) obtained voluntary survey data for specific information; and (3) then crafted this into new formats and analyses. Even in the case where a provider voluntarily gives information to a report-

---

[11]California Health Care Market Report 2004, at 3, available at http://www.chcf.org/topics/view.cfm?itemID=101693.

[12]California Health Care Market Report 2004, at 24, available at http://www.chcf.org/topics/view.cfm?itemID=101693.

[13]California Health Care Market Report 2004, at 2, available at http://www.chcf.org/topics/view.cfm?itemID=101693.

[14]http://www.nyshaf.org/index/hmo__report__card.

[15]"New York State HMO Report Card," at 7, http://www.nyshaf.org/index/hmorc-data-sources.

ing entity, once reported to the public, that information loses any proprietary character it might have had prior to disclosure.

§ 5:9 Third-party uses of information—Report cards—Advertising

Similar to quality-focused public reporting efforts, providers and health plans may use information of this sort in advertising their own services to the public. It is becoming increasingly common for providers to track their own outcomes data or other quality information for disclosure in advertising campaigns. A provider itself may voluntarily offer information to the public, or an entity with which it contracts (such as a health plan) may collect information on its own and distribute this information to the public. Likewise, a competitor may wish to advertise its own quality in comparison to the provider's quality, thereby offering evidence that the competitor is superior to the provider. The competitor may use information already in the public domain.

For example, in 1997, Aetna/US Healthcare ran an advertisement in the Philadelphia Inquirer stating "There are a number of reasons why Philadelphians have made Aetna U.S. Healthcare #1." Although the ad listed several factors, the most interesting use of data appears in a small chart outlining "HMO Enrollment in Philadelphia Area." The advertisement indicates that the data was taken from the Pennsylvania Department of Health, from figures published September 30, 1996 for Bucks, Chester, Delaware, Montgomery, Philadelphia "and other contiguous counties." The advertisement further indicates that not every company operated in every county. Aetna/U.S. Healthcare is naturally at the top of the chart, with a figure of 980,787.[1] Keystone East, Health Partners, Prucare Philadelphia, and CIGNA are each listed below, obviously with much lower figures.

The implication of the advertisement is obvious—Aetna/U.S. Healthcare *must* be the best HMO in the region, because it has the highest numbers, thereby making it "#1."

[Section 5:9]

[1]Interestingly, the advertisement does not explicitly state that this is the number of enrollees.

Although the source of the information is only indicated as "Pennsylvania Department of Health," the logical inference is that the figures were gleaned from the same data set used by the Department in the creation of its HMO report cards.

Of course, not all comparative advertisements will explicitly mention competitors. Some may only offer comparisons to regional or national averages. For example, Atlantic Health System ran an advertisement noting that Morristown Memorial Hospital (a hospital within Atlantic's system) was "One of the country's most successful cardiac surgery programs." The advertisement included four vertical bars indicating open-heart surgery survival rates, and which placed Morristown Memorial Hospital at the highest rate of the four, with 94.37%. However, rather than comparing this rate to other competitors, the rate was compared to "New York" at 92.68%, "National Average" at 91.64%, and "New Jersey" at 90.73%. The source of the data given in the advertisement was a 1-year survival rate for coronary artery bypass grafts ("CABG"), based on HCFA data, using the average of CABG with catheterizations and without catheterizations.

In this advertisement, while no competitor is named, the source of information is still presumably public information. Certainly, by virtue of the advertisement being published, the information is being made public, even if it is not necessarily in the form in which it appears in the source materials. Thus, any provider from whom data was collected (which, in this case, would include every provider performing CABG in the nation) is, at least indirectly, having data about them being used by a third party.

Other types of advertisements may make no explicit comparison whatsoever, and may simply assert that the advertising party is "the best" or "#1." However, in many cases, they may base such claims on public reports or data. For example, Columbia-Presbyterian Hospital in New York published an advertisement in the New York Times.[2] Stating, "There are a lot of smart hospitals in New York. But only Columbia-Presbyterian made the honor roll."[3] It then points out that in the "tri-state area" (which is not defined),

[2]New York Times, at A9 (Sept. 23, 1997).

[3]New York Times, at A9 (Sept. 23, 1997).

Columbia-Presbyterian Medical Center was the only hospital to earn U.S. News & World Report's "Honor Roll" for cardiology, gynecology, pediatrics, psychiatry, and neurology, "among others."[4] In this advertisement, even without referring directly to other providers, Columbia-Presbyterian is indicating its superiority, based on public data, originally published by U.S. News and World Report. There are, of course, implicit comparisons being made.

The point of the advertising is obvious: it offers the consumer proof that the advertising entity has been recognized by an authority in the field, or presents the consumer with concrete data from which the consumer can draw only one obvious conclusion—that the advertising entity is the best or offers the highest quality care. However, in each instance the critical information, whether from the government, the accolades of a private entity engaged in quality ranking, or some other source, which has been gathered to substantiate the rating, prior to disclosure, might have been considered "proprietary." By virtue of its publication, in the original source for the data, or in the actual advertisement itself, that information is now a matter of public record and loses what proprietary status might previously have attached.

§ 5:10 Third-party uses of information—Report cards—Commercial purposes

Data may also be traded commercially, often for purposes such as market research. A variety of entities provide databases or clearinghouses of healthcare data in today's marketplace collecting data from public sources, such as state health agencies, and also through contracts with other organizations that have either themselves collected or been given access to data by providers.

IMS Health provides what it describes as "pharmaceutical market intelligence" to drug companies.[1] IMS states that it "receives data from more than 29,000 data suppliers cover-

---

[4]New York Times, at A9 (Sept. 23, 1997).

[Section 5:10]

[1]http://www.imshealth.com/ims/portal/front/indexC/0,2478,6599__1825,00.htm. IMS notes on this same page that "Just about every major pharmaceutical and biotech company in the world is a customer of IMS."

ing 225,000 data sites around the world."[2] Its data sources include drug manufacturers, wholesalers, retailers, pharmacies, mail order, long-term care facilities and hospitals, as well as trade and professional associations such as the American Medical Association.[3] The information collected is used to produce a range of information products for pharmaceutical companies to assist them in their own marketing efforts. For example, IMS' Xponent product line is a set of data products that track prescription activity on a prescriber-by-prescriber basis.[4] Xponent data is compiled from retail pharmacies, mail-order pharmacies, and long-term care pharmacies.[5] IMS' DDD database covers 90% of the pharmaceutical market by tracking direct and indirect sales throughout the chain of distribution, including hospitals, clinics, mail-order services, food stores, and other sources.[6] Commercialization of this data through the various IMS products accounts for approximately 60% of IMS' annual revenues.[7]

Although not its primary business, WebMD also engages in commerce in data. In general, WebMD provides electronic information transmission services and practice management tools to providers. For example, WebMD offers WebMD Envoy, a software suite that allows for electronic transactions between providers, payors, pharmacies, and other businesses in the healthcare industry.[8] However, WebMD also sales de-identified information to third parties. In analyzing its business risks with respect to the HIPAA Privacy Rules, in its Securities and Exchange Commission Group WebMD

---

[2]http://www.imshealth.com/ims/portal/front/articleC/0,2777,6599__18731__40198214,00.html.

[3]http://www.imshealth.com/ims/portal/front/articleC/0,2777,6599__18731__40198214,00.html; IMS 10-K annual SEC report, at 4 (March 10, 2004), available at http://ir.imshealth.com/phoenix.zhtml?c=67124&p=irol-sec. Note that IMS specifically licenses access to and sub-licensing rights for the AMA physician database.

[4]http://www.imshealth.com/ims/portal/front/articleC/0,2777,6599__18731__43204559,00.html.

[5]IMS 10-K, at 3.

[6]http://www.imshealth.com/ims/portal/front/articleC/0,2777,6599__18731__43204559,00.html.

[7]IMS 10-K, at 2.

[8]WebMD 10-K annual SEC filing, at 4 (March 15, 2004), available at http://www.webmd.com/corporate/index.html.

indicated "[The HIPAA Privacy Rules] may adversely affect our ability to generate revenue from the provision of de-identified information to third parties."[9] Moreover, from 2000 to 2002, WebMD provided de-identified information to Quintiles, a company providing strategic research and clinical development services, pursuant to a data use agreement.[10] Under the agreement, the following two definitions applied:

> "LICENSED DATA" means all of the following transmitted to, from, or through or otherwise received, possessed or controlled from time to time by or for the benefit of Healtheon to the extent Healtheon is not prohibited by applicable Law or contractual arrangement from providing such data to Quintiles under this Agreement, regardless of the medium of or circumstances giving rise to transmission: (1) Transaction Data and (2) other data concerning (A) the health, medical condition, or treatment of actual, specific people, (B) the behavior of actual, specific people intended to treat, maintain, or otherwise influence their health or medical conditions, or (C) the providing of health care or reimbursement or payment therefor with respect to actual, specific physicians, hospitals, health maintenance organizations, governmental entities, and other providers, pharmacies, and payors.
>
> "DE-IDENTIFIED DATA" means Licensed Data that has been through the De-Identification process. For the avoidance of doubt, De-Identified Data only de-identifies data elements that make the Licensed Data individually identifiable to a particular patient or consumer (unless other elements of the Licensed Data are required by Law to be de-identified), and those data elements (other than patient or consumer identifying data) of the Licensed Data that are not required to be de-identified constitute De-Identified Data notwithstanding their identifiable format. By way of example, and without limitation, specific identifiable data such as the names of specific pharmacies, physicians, hospitals and payors constitute De-Identified Data once the corresponding Licensed Data has been through the De-Identification process, provided that such items are not required by Law to be de-identified. Licensed Data will also be considered De-Identified Data for purposes of this Agreement if the particular data set does not contain patient or consumer identifying data or any data elements that require de-identification pursuant to applicable Law and, accordingly,

---

[9]WebMD 10-K annual SEC filing, at 34 (March 15, 2004), available at http://www.webmd.com/corporate/index.html.

[10]WebMD 10-K annual SEC filing, at F-19 (March 15, 2004), available at http://www.webmd.com/corporate/index.html.

such data set does not go through the De-Identification process.

The agreement granted to Quintiles a perpetual, worldwide, irrevocable license to use de-identified Licensed Data, as well as the right to sell, license, and otherwise commercialize the data and to develop products using the data.[11] In exchange, Quintiles would pay WebMD royalties based on Quintiles' revenues from the use of the data.[12] The major benefit to Quintiles is that it could use the data in providing services to pharmaceutical companies. Although the agreement is no longer in effect, it offers a clear example of how entities have begun to use data in commerce.

Another database, the Massachusetts Health Data Consortium ("MHDC"), collects data from a variety of sources. For example, the MHDC's inpatient discharge database draws information from the Massachusetts Division of Healthcare Finance and Policy, after which the MHDC "enhances the data into a population-based file ensuring 100% resident-based provider-specific information."[13] The MHDC sells its data, allowing purchasers to customize reports along any of the 32 data elements tracked in the inpatient database.[14] Purchasers must also sign a Data Use Agreement, which restricts the purchaser from disclosing purchased data, except for reasons specified in the agreement. However, the agreement does not prohibit the resale of such data, provided that the intent to resell is disclosed in the agreement and that the data as resold is deidentified.[15]

With each of the commercial examples listed above, data at least partially generated by providers, is being commercialized. In the current marketplace, data has significant value beyond merely providing transparency or evidence of quality to consumers. Providers need heightened

---

[11]Data Use Agreement, § 2.1.

[12]Data Use Agreement, § 2.3.

[13]http://www.mahealthdata.org/data/inpatient/index.html.

[14]These elements include: hospital name and location; patient sex; patient age; total length of stay; admission type; diagnosis related group; as well as others. *See* http://www.mahealthdata.org/data/inpatient/elements.html.

[15]MHDC Data Use Agreement, Section II.I, Schedule I.B, available at http://www.mahealthdata.org/data/DataUseAgreement.pdf.

sensitivity to the economic value of their data and therefore their need to maintain control over it.

§ 5:11 The contractual context: How providers lose control over proprietary information

Once a provider turns information over to another party, be it a health plan, state agency, quality-tracking private entity, marketing entity, or the public itself through an advertising campaign, the provider loses much of its ability to control the information. At best, the provider now shares control with another entity; at worst, the provider's data has become public record and is free for all to use. Without explicit contractual attention, a provider will typically lose control of its data when it is in play through a contractual relationship with another party.

When entering into a contractual relationship, a provider may be required to relinquish control of certain proprietary data as a condition of signing the contract itself or by permitting that entity rights to its proprietary data ranging from mere access to full ownership. In certain instances a contracting party will affirmatively assert transfer of the other party's otherwise proprietary information. For example, in a provider contract with a physician group, a major insurance company has defined *its* "Proprietary Information" as:

> Any and all information, whether prepared by a party, its advisors or otherwise, relating to such party or the development, execution or performance of this Agreement whether furnished prior to or after the Effective Date. Proprietary Information includes but is not limited to, with respect to Company, the development of a pricing structure, (whether written or oral) all financial information, rate schedules and financial terms which relate to Group and which are furnished or disclosed to Group by Company.

Under the contract, the Group is required to further release medical information and records, as well as encounter data to the Company. Although the agreement in question contains a clause by which the parties were not permitted to disclose to a third party without consent (except in cases where such disclosure was required by law), the implications of such a broad definition of "Proprietary Information" are considerable. Even without the ability to disclose, as written, this granted the Company access to "any and all information

relating to such party." The breadth of this assertion is virtually unlimited, and by implication could transform the Group's data (*e.g.,* numbers of its patients insured by Company, incidence of specific medical conditions among its patients insured by Company) into the Company's. In the absence of a savings clause (*e.g.,* "Notwithstanding this provision, Group shall at all times retain ownership of data relating to it and arising out of this Agreement"), the Group loses the ability to use such data itself.

And what if the limitation on disclosure had not existed? In such circumstances, the Company might have been able to further disclose the information to third parties. The Company could have sold the information to a company like IMS Health, it could have used specifically identified information about the group in advertising materials, or it could have disclosed such information to a commercial report care publisher. In the standard terms of a different provider agreement with a hospital, another MCO included language claiming ownership of "any information gathered or provided regarding the cost and utilization of health care services by Members (whether Member specific, account specific or aggregate) or software data." The hospital would be prohibited from disclosing such information without the prior consent of the MCO, although the MCO "[could] use and/or include data generated by [the hospital] for studies and reports (including reports to its customers) on a customer-specific or aggregate basis."

In this example, the insurer both asserts ownership of information that could otherwise be considered the hospital's proprietary information, and claims the right to further disclose such information while denying the hospital any such rights. There is also no requirement that the insurer obtain the hospital's consent before disclosing any such information. Thus, the provider has lost most of its rights to control the use of information by virtue of the contract's language.[1]

[Section 5:11]

[1]Even a well-drafted contract may still require disclosure of certain information due to requirements under the law. For example, both the provider itself and the other party may be required to disclose information to state health agencies. Thus, even a narrowly drafted contract may still include a provision permitting disclosure of otherwise confidential or pro-

§ 5:12 Risk control for provider data: Effective contract drafting

Given that providers can accumulate a wide range of data, much of which is attractive to parties seeking to use and/or disclose that data, it is important for providers to understand how best to protect themselves and their data. Ideally, a provider will protect itself through carefully drafted contract language. However, this chapter will also provide examples of statutory protections to keep in mind when drafting such language.

§ 5:13 Risk control for provider data: Effective contract drafting—Contractual Methods

This chapter will discuss five principal approaches to contractual protection of a provider's proprietary data. These are: (1) confidentiality clauses; (2) intellectual property ownership clauses; (3) right to challenge clauses; (4) right to review clauses; and (5) an ownership "savings" clause.

§ 5:14 Risk control for provider data: Effective contract drafting—Contractual methods—Confidentiality Clauses

Confidentiality clauses allow a provider to control the ability of the parties to disclose a wide range of information, including the actual existence of the agreement, the proprietary information discussed in this chapter, or other information agreed to be confidential. Confidentiality clauses can be worded broadly or they can be narrowly tailored to only a few essential data.

For example, the following language is taken from a contract between a behavioral health network and a prospective hospital provider, in which the hospital provider was to become a member of the network. Although originally worded to protect the confidentiality of information transmitted from the network to the provider, the language was extended to protect the provider's data.

(1) Provider and Network hereby acknowledge and agree

---

prietary information "as required by law." However, this still would not apply to voluntary disclosures such as advertising, commercialization of the data, or disclosure to a private entity such as the Leapfrog Group.

that in the course of their relationship under this Agreement, Provider shall disclose to Network certain Confidential Information, as hereinafter defined, which the parties acknowledge and agree is proprietary and valuable to Provider. Network hereby agrees to treat such Confidential Information in accordance with the provisions of this Agreement and to take or refrain from taking the actions set forth herein with respect to the Confidential Information.

(2) For purposes of this Agreement, the term "Confidential Information" means any and all information, in whole or in part, and in whatever form or medium, furnished to Network by or on behalf of Provider or created by Provider pursuant to this Agreement, including but not limited to data and/or information relating to Provider's business, and any and all professional and business practices, strategic plans, trade secrets, financial statements, financial information, contractual provisions, business plans, marketing plans or materials, business or clinical protocols or templates, contact lists, sources of business, software programs, copyrighted materials, or other proprietary information. Confidential Information does not include information which Network can demonstrate (i) is generally available to or known by the public other than as a result of disclosure by Network or (ii) was obtained by Network from a source other than Provider, provided that such source is not bound by a duty of confidentiality to Provider or another person or entity with respect to such information.

(3) Network agrees that it:

(i) shall use Confidential Information solely in the course of its relationship with Provider;

(ii) shall not use Confidential Information to compete with or to the detriment of Provider or its affiliates;

(iii) shall keep the Confidential Information strictly confidential and, except as authorized by the terms of this Agreement, will not disclose or distribute the Confidential Information to any person or entity without the prior written consent of Provider. Provider may disclose Confidential Information to such of its directors, officers, employees and agents (the "Representatives") who need to have the Confidential Information to evaluate whether to enter into a business relationship with Network, so long as those Representatives agree to be bound by the terms of this Section of the Agreement, and then only to the extent necessary to such evaluations. Provider shall be responsible for any breach of this Section of the Agreement by its Representatives.

(4) In the event that Network is or its Representatives are requested or required (by oral questions, interrogatories,

> requests for information or documents in legal proceedings, subpoena, court order, civil investigative demand or other similar process) to disclose any of the Confidential Information, it shall provide Provider with prompt written notice of any such request or requirement so that Provider may seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this Agreement. If, in the absence of a protective order or other remedy or the receipt of a waiver in accordance with this Agreement, Network is nonetheless legally compelled to disclose Confidential Information to any tribunal, regulatory authority, agency or similar entity, Network may without liability hereunder or under other applicable law, disclose to such tribunal, regulatory authority, agency or similar entity, only that portion of the Confidential Information which is legally required to be disclosed, provided that it exercises reasonable efforts to preserve the confidentiality of the Confidential Information.

The first portion merely sets out that the relationship created by the overall agreement will necessarily involve the exchange of confidential information. The second portion, however, provides a broad definition for "Confidential Information." This section includes both materials that would otherwise be protected by statute (*i.e.*, trade secrets, copyrighted materials, software programs) and material that might not be protected by statute or even common law (*i.e.*, contact lists, marketing materials, sources of business, and "other proprietary information."). This second portion is intentionally drafted to be inclusive, but not limited to the materials described in the definition. In drafting such a clause, providers should consider what types of information may be disclosed by virtue of the relationship and tailor the definition section accordingly. Alternatively, the provider may take a "kitchen sink" approach, and simply attempt to include any and all types of information that the provider wishes to protect, regardless of whether the provider anticipates sharing it during the course of the agreement.

The third portion outlines the permissive uses of the information, restricts disclosure for any purpose not authorized by the agreement, and requires all other disclosures to be given prior written permission by the Provider. The practical effect of such language would be, for example, to restrict the network from selling data culled from confidential information gathered from the provider to a third party such as IMS or the Massachusetts Healthcare Data Consortium. If the network were to use the information in such a manner, it would constitute a breach of the agreement.

However, the fourth portion creates an exception for disclosures required by law. This explicitly includes disclosures both for court proceedings, and to state agencies or regulatory authorities. Thus, it would permit disclosures by the network to, for example, a state department of health pursuant to requirements relating to a state healthcare report card program.

The key advantage to confidentiality language in agreements is that they provide clear contract language that a court may use to protect a provider's data, even if such data is not subject to statutory protection. For example, in *Medical Broadcasting Company v. Flaiz*,[1] Medical Broadcasting Company ("MBC") was a provider of business services to health care and pharmaceutical companies, which had sued its former employee Flaiz for disclosing certain information, including business methodologies and materials protected by the Digital Millenium Copyright Act, in breach of a confidentiality agreement signed when Flaiz was an employee. Flaiz, having lost at trial, challenged the award of damages, and argued that the court incorrectly instructed the jury. Claiming the court should have instructed the jury that he could not be held liable if he only disclosed information that was generally known in the trade, even if it was not generally known to the public.[2] In response, the court made two noteworthy comments. First, "While employee covenants not to compete are subject to a rule of reason as to time and space, confidentiality restrictions are not subject to such a limitation."[3] Second, the court stated that, "If information is generally known in the trade, it necessarily follows that it is in the public domain and thus generally available to the public . . . . The terms ["public" and "in the trade"] are in essence synonymous, at least in this case."[4] Consequently, because the jury had found that none of the information

---

[Section 5:14]

[1]Medical Broadcasting Co. v. Flaiz, 2003 WL 22838094 (E.D. Pa. 2003).

[2]Medical Broadcasting Co. v. Flaiz, 2003 WL 22838094, at *2 (E.D. Pa. 2003).

[3]Medical Broadcasting Co. v. Flaiz, 2003 WL 22838094, at *3 (E.D. Pa. 2003).

[4]Medical Broadcasting Co. v. Flaiz, 2003 WL 22838094 (E.D. Pa. 2003).

disclosed was in the public domain, Flaiz's motion to set aside the verdict was denied.[5]

The business methods in *Flaiz* were not protected under the Digital Millenium Copyright Act, and the court did not discuss any other statutory protections that might have been available. Instead, the court focused solely on the breach of the confidentiality clause. While the methodologies might have been protected under state trade secret laws or some other statute, the language of the confidentiality clause controlled. This is especially significant in light of the court's note that confidentiality clauses are not subject to time and space restrictions. Thus, a well-drafted confidentiality clause can protect a wide variety of materials indefinitely.

In certain circumstances, even an unsigned confidentiality agreement will be binding. In *AutoMed Technologies, Inc. v. Eller*,[6] AutoMed, a company in the business of designing automated medical dispensing systems, sued Eller for disclosure of certain confidential information after Eller went to work for a competitor. Eller, however, argued that he had never signed the addendum to his employment agreement, and filed a motion to dismiss for failure to state a claim. However, when Eller had originally been offered employment by AutoMed, he had been sent a letter which included language reading, "Finally, your choice of employment with AutoMed will require you to complete a revised Non-Competitive and Non-Disclosure Agreement. A copy of this Agreement is attached as Exhibit A."[7] Although Eller signed the letter of engagement, he did not also sign Exhibit A.[8] The court found that, because Eller had continued to work, and because the letter had explicitly conditioned employment on agreeing with the terms of the confidentiality clause, his conduct indicated that he had agreed to the terms, and

---

[5]Medical Broadcasting Co. v. Flaiz, 2003 WL 22838094 (E.D. Pa. 2003).

[6]AutoMed Technologies, Inc. v. Eller, 160 F. Supp. 2d 915 (N.D. Ill. 2001).

[7]AutoMed Technologies, Inc. v. Eller, 160 F. Supp. 2d 915, 924 (N.D. Ill. 2001).

[8]AutoMed Technologies, Inc. v. Eller, 160 F. Supp.2d 915, 924 (N.D. Ill. 2001).

they were enforceable, regardless of the fact that Eller had never signed.[9]

The potential strength and protection of confidentiality clauses makes them the ideal choice for a provider's "first line of defense," since a well drafted clause can provide significant protection to the provider's data. Although many contracting entities may be unwilling to accept restrictions or conditions of the sort described above, the language can at least prove a useful guide in what to request during negotiations.

§ 5:15 Risk control for provider data: Effective contract drafting—Contractual methods—Intellectual property ownership clauses

An intellectual property ownership clause is also often a useful complement to a confidentiality clause. Asserting ownership of intellectual property may include ownership of copyrights, trademarks, patents, trade secrets, or other proprietary data. An ownership clause is useful in that it expresses the intent and understanding of the parties that only one of the parties owns or has rights to use and disclose the intellectual property in question. This serves a dual purpose, practically speaking. First, it erases any doubt ahead of time as to the rights of the respective parties insofar as the intellectual property is concerned; without such a clause, it is possible that one party may believe that, by virtue of having entered into the relationship, it may have some rights to intellectual property that the other party never intended to grant. Second, should litigation occur, such a clause is evidence of the parties' mindset at the time the agreement was signed. This can effectively prevent an opposing party in litigation from asserting that it had any ownership interest in the intellectual property covered by the clause; when the plain language of the agreement runs counter to such an argument, a judge will be less likely to uphold such a claim (or counterclaim), and it may be easier to dismiss in pretrial motions. When coupled with a confidentiality clause, these two clauses can close off means by which a contracting party may attempt to use, control, or disclose proprietary information.

---

[9]AutoMed Technologies, Inc. v. Eller, 160 F. Supp.2d. 915, 924-25 (N.D. Ill. 2001).

For example, the following language is taken from a confidentiality agreement between a provider and a practice management company. Although the language is worded to protect the manager, the positions can easily be switched to favor the provider, or the language could be changed to provide mutual protection.

> A. Recipient acknowledges that Manager is the owner of the name [Insert Manager's Trademark], (the "Mark"). Except as expressly set forth in this Agreement, Provider shall make no use of the Mark without the express prior written approval of Manager. Each use of the Mark pursuant to this Agreement shall require prior approval by Manager. Each use of the Mark shall specifically and conspicuously note the ownership by Manager.
>
> B. Provider acknowledges that Manager is the owner of any and all works previously created by or on behalf of Manager which fall within the scope of the 1976 Copyright Act (the "Act"). (17 U.S.C.A. §§ 101, et seq.) Any such materials (the "Works") are protected under the Act.
>
> C. Provider acknowledges Manager's exclusive right, title, and interest in and to the Marks and Provider shall not at any time do or cause to be done any act or thing contesting or in any way impairing or tending to impair any part of such right, title, and interest in connection with the Mark and the Works. Provider shall not in any manner represent that it has any ownership in the Mark or the Works and Provider acknowledges that use of the Marks and reprinting of the Works shall not create in the Provider's favor any right, title, or interest in or to the Mark but all uses of the Mark by the Provider shall inure to the benefit of Manager. And, Provider shall at no time adopt or use, without Manager's prior written consent, any word or mark which is similar to or likely to be confused with the Mark.
>
> D. Every use of the Mark and the Works by Provider shall inure to the benefit of Manager. At no time shall Provider acquire any rights in the Mark or the Works by virtue of any use they may make of any of them.

The language above only addresses uses of trademarks and copyrighted materials, but could also be expanded to claim ownership of materials covered under patent law, trade secrets, or other proprietary information. Confidentiality and intellectual property clauses generally favor one party over the other and require negotiating power to obtain. Where the other side is stronger, as in an MCO-provider negotiation, the next two mechanisms may prove more useful.

§ 5:16 Risk control for provider data: Effective contract drafting—Contractual methods—Right to Challenge Clauses

Right to challenge clauses offer the provider some limited ability to control how information is disclosed or whether it is disclosed at all. Generally, a right to challenge clause will be the stronger of the two and the more beneficial to the provider. A right to challenge clause permits the provider to review information that the other party intends to publish, disclose, or otherwise use, and grants the provider the ability to challenge the accuracy of the information. Depending on how the clause is worded, this may require the disclosing entity to revise the statement to be more accurate.

> Except as otherwise required by law or regulation, [Disclosing Party] shall present Provider with a sample of any disclosure specifically mentioning Provider, or which uses Provider data, not less than fifteen (15) days before the anticipated disclosure. If Provider reasonably determines the disclosure to be false, inaccurate, or potentially detrimental to Provider's legitimate business and confidentiality interests, Provider shall notify [Disclosing Party], and [Disclosing Party] shall not disclose the material. Provider shall not unreasonably withhold its consent to disclose, and shall make all reasonable efforts to provide [Disclosing Party] with alternative language that is acceptable to Provider.[1]

A clause of this nature actually benefits both parties. On the provider side, there is a greater ability to prevent erroneous information from being disclosed, and thus protect the provider's interest. On the disclosing entity's side, the right to challenge clause acts as an internal quality control mechanism and may help the disclosing entity avoid a future lawsuit over the disclosure; if the provider was given the right to challenge but waived that right, the disclosing entity may be able to prevent the provider from sustaining a claim for misrepresentation. In the specific clause above, the language is also worded so that the Provider must at least attempt to provide the Disclosing Party with alternative language. The benefit of including such language is twofold:

[Section 5:16]

[1]The actual time frames used should, of course, be adjusted to fit the circumstances of the parties. In some situations, fifteen days might be too much or too little time for review.

first, in "time crunch" situations, this requirement may provide a faster means of resolving differences over the disclosure; second, assuming the alternative language is acceptable to both parties, it offers the Disclosing Party protection from future liability to the Provider, because the Disclosing Party is using language that the Provider has already approved.

§ 5:17 Risk control for provider data: Effective contract drafting—Contractual methods—Right to Review Clauses

The right to review clause is a somewhat weaker version of the right to challenge clause. This clause permits the provider to merely view what will be disclosed prior to such disclosure, but does not permit the provider any ability to prevent the disclosure. If the provider is unable to secure a right to challenge clause due to weak relative bargaining power, a right to review clause may be more palatable for "Goliath." At least both parties will know what will be disclosed, even if the provider lacks the ability to prevent such disclosure.

> Provider reserves the right to review any and all disclosures of data made available by Provider to [Insert other party here]. No less than ten (10) days prior to such disclosure, [other party] shall present Provider with a copy of the anticipated disclosure for review.

However, if neither a right to challenge nor a right to review clause is acceptable to the disclosing entity, a provider may at least request that the agreement include a specifically limited definition of the disclosures the disclosing entity intends to make. If the disclosing entity is unwilling to limit itself prospectively in terms of the disclosures it may make, it may still be willing to identify within the agreement those that it knows it will make.

> During the term of this Agreement, [Other Party] may use information gathered from Provider in disclosures for [anticipated usage 1], [anticipated usage 2], and [anticipated usage 3].

The agreement should already include a definition of what information will be used; without such a definition, this clause will not be anywhere near as useful, because it will not give the provider any better understanding of what will be disclosed than the provider had before inclusion of such language in the agreement.

§ 5:18 Risk control for provider data: Effective contract drafting—Contractual methods—"Savings Clauses"

As a final mechanism to protect provider data, consider using a "savings clause." A "savings clause" attempts to claim ownership of the provider's data, even though the provider may have no control over its disclosure under the agreement. For example, if the other contracting party refuses to be restricted in its ability to disclose and/or otherwise use a provider's data, a "savings clause" will at least indicate that the parties agree that the provider still owns the information, regardless of the uses made by the other party during the term of the agreement. Such language could be drafted as follows:

> Notwithstanding the foregoing, Provider and [Other Party] agree that the following properties or information remain the exclusive property of Provider: [list properties/data]. [Other Party] is hereby permitted to use [Provider's properties/data] for the purposes stated in this Agreement [and for any other commercially reasonable purposes], provided that [Other Party] does not use [Provider's properties/data] to compete with or disparage Provider. [Other Party] shall cease usage of [Provider's properties/data] upon termination of this Agreement.

The primary advantage of employing such a clause is that it clearly states what is and remains the provider's property. There is no question as to ownership of the data, and the other party cannot continue to use the information after the agreement terminates. In addition, the non-competition and disparagement language (as well as, to a lesser extent, the "commercially reasonable uses" language) provide language that the provider may use to, at least in a limited sense, control the other party's use of the information; if the other party disparages or competes with the provider, or uses the provider's information for commercially unreasonable purposes, the provider would have a reason under the contract to challenge and prevent such uses.

§ 5:19 Risk control for provider data: Effective contract drafting—Statutory Protections

An understanding of statutory protections is useful in two contexts. First, statutory protections for information offer providers a means of controlling such information when no

contractual relationship exists between the provider and the party attempting to use the information. Second, although statutory protection does not need to be invoked within the body of the contract in order to obtain the protections of the statute, to the extent possible, it may prove helpful to specify which statutes explicitly apply to the information covered by the contract.[1] The statutes discussed herein will not always apply to both situations, but will still be useful to know what protections are available and in which settings they will apply. Finally, following the statutes do not represent the definitive list of statutory protections available for data. Rather, they are provided merely for guidance and as examples of statutes that may be used to protect data.

§ 5:20 Risk control for provider data: Effective contract drafting—Statutory protections—Federal statutes—Copyright law

In general, providers will have little need to seek protection under federal copyright law. Typically, the only reason that a provider will want to focus on copyright is because the provider expects to publicize the information itself in a medium to which copyright law applies.[1] For example, a provider may want to prohibit a party with which it is contracting from using the information in question (*e.g.,* in negotiating for higher payment rates the provider submits to the MCO a chart demonstrating its cost savings by comparison with hospital services), or from publishing the information before the provider has a chance to. In general, an original selection and arrangement of factual information or data will be copyrightable.[2] However, raw data (such as surgical outcomes, prescription trends, etc.) will not qualify for

---

[Section 5:19]

[1]However, in doing so, the drafter should remember to use the phrase "including, but not limited to," so as to remove the possibility that the other party might claim failure to explicitly include a given statute as a waiver of the first party's rights under that statute.

[Section 5:20]

[1]17 U.S.C.A. § 102(a) applies to "original works of authorship fixed in any tangible medium of expression," and includes literary, pictorial, graphic, or audiovisual works, and sound recordings.

[2]17 U.S.C.A. § 102(b). *See also* Feist Publications, Inc. v. Rural Telephone Service Co., Inc., 499 U.S. 340, 348-49, 111 S. Ct. 1282, 113 L.

copyright protection in and of itself.[3] Thus, a provider will only have remedies available if the *expression* of the data is copied, rather than the raw data itself. In other words, in order to claim copyright infringement with respect to data, the infringing party would have to essentially take a snapshot of the page or medium in which the data appeared and reproduce it, since the raw data would not be protected under copyright law.

However, the remedies afforded by copyright law are considerable. A provider who copyrights data may sue an infringer to obtain an injunction preventing publication, and may obtain compensation of up to three times the damages. Thus although it is rare that a provider will seek refuge in federal copyright law, to the extent possible, providers should consider using it.

§ 5:21 Risk control for provider data: Effective contract drafting—Statutory protections—Federal statutes—Lanham Act and Federal advertising laws

In general, the Lanham Act, which governs federal trademark law, will not be useful for protecting against misappropriation of data. The Lanham Act primarily controls how trademarks are to be used in interstate commerce, and thus would not be relevant in a case where, for example, a provider attempted to sue a third party for improperly obtaining proprietary information. However, as it relates to advertisements, the Lanham Act may prove a useful tool for a provider seeking to protect itself from improper public characterization by a competitor.

Section 43(a) of the Lanham Act prohibits the use of words, terms, names, symbols, devices, or combinations thereof, or false designations of origin, false or misleading descriptions of fact, or false or misleading representations of fact in

---

Ed. 2d 358 (1991) (copyright did not extend to facts contained in a telephone book, but could extend to an original selection or arrangement of such facts).

[3] 17 U.S.C.A. § 102(b).

commerce.[1] If it is proven that such actions misrepresent "the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities," the misrepresenting party will be civilly liable.[2] A person who violates these provisions may be subject to injunctive relief, and may have to pay the plaintiff's damages, disgorge profits, and even pay the cost of litigation, subject to the determination of the court and principles of equity.[3]

Health care plans have used the Lanham Act to sue each other for violations of § 43(a) in advertising. In *U.S. Healthcare, Inc., v. Blue Cross of Greater Philadelphia*,[4] both U.S. Healthcare and Blue Cross ("BCGP") engaged in activities implicated by the § 43(a) of the Lanham Act. Each company, in several advertising campaigns, made various statements about its own products and about the competitor's products. The case provides excellent examples of the types of advertising that will trigger the Lanham Act's prohibitions, and which advertisements will not.

BCGP ran several advertisements in print media, on television, and on the radio, as did U.S. Healthcare. Consider the following:

> Three television advertisements run by BCGP were essentially "identification pieces," with no real substantive information. The advertisements included a statement "Better than [U.S. Healthcare]. So good, it's Blue Cross and Blue Shield." The court stated, "This strikes us as the most innocuous kind of 'puffing' and presents no danger of misleading the consuming public. Consequently, we find that no cause of action lies with regard to these three advertisements."[5]
>
> Another BCGP television advertisement factually represented that BCGP's own product (the Personal Choice PPO) covered "routine doctor visits, prescriptions, even pediatric care." A question was raised as to whether Personal Choice actually

---

[Section 5:21]

[1]15 U.S.C.A. § 1125(a)(1).

[2]15 U.S.C.A. § 1125(a)(1)(B).

[3]15 U.S.C.A. § 1117(a).

[4]U.S. Healthcare, Inc. v. Blue Cross of Greater Philadelphia, 898 F.2d 914 (3d Cir. 1990).

[5]U.S. Healthcare, Inc. v. Blue Cross of Greater Philadelphia, 898 F.2d 914, 926 (3d Cir. 1990).

> covered check-ups as "routine doctor visits," and thus, whether BCGP had misrepresented its own product. Although the court did not issue a ruling as a matter of law, it did state that there was a sufficient question regarding the misrepresentation to potentially give rise to a cause of action under the Lanham Act.[6]
>
> One of the print advertisements described U.S. Healthcare's referral procedure, indicating that after a subscriber selected a primary care physician, that physician would have to grant permission for the subscriber to be examined by a specialist. However, the advertisement went on to state "You should also know that through a series of financial incentives, [U.S. Healthcare] encourages this doctor to handle as many patients as possible without referring to a specialist. When [a U.S. Healthcare] doctor does make a specialist referral, it could take money directly out of his pocket. Make too many referrals, and he could find himself in trouble with [U.S. Healthcare.]."

The Lanham Act may be useful for a provider who has been unfairly and improperly characterized by a competitor in advertising. If, for example, a competitor mischaracterized publicly available data, such as a state's report card results, the provider who had been so maligned could bring suit against the competitor. In circumstances involving advertising where the information portrayed would be considered public, the Lanham Act may provide one of the only means of controlling the expression and presentation of data. However, outside of clauses controlling the use of trademarks, there will not generally be any reason to mention the Lanham Act within the body of a contract. Rather, the Lanham Act will be most useful when the provider has no contractual relationship with the party mischaracterizing data about the provider.

§ 5:22 Risk control for provider data: Effective contract drafting—Statutory protections—State Laws—State Peer Review Protection

At the state level, peer review protection acts, state rights to privacy or publicity, or trade secret law may come into play. Every state has its own version of Peer Review Protec-

---

[6]U.S. Healthcare, Inc. v. Blue Cross of Greater Philadelphia, 898 F.2d 914, 926 (3d Cir. 1990).

tion, although they provide different levels of protection.[1] Providers sometimes seek to refuse disclosure of data because it would breach their statutory protection. Unfortunately while there may be a rare instance in which this will work, these statutes are fairly limited in terms of what they protect and when. In California, a provider is entitled to protect peer review information and prevent its disclosure, but the statute only focuses on discovery in the course of pre-trial litigation and does not address other instances of disclosure.[2]

Pennsylvania's Peer Review Protection Act provides similar protections, although they too are focused on a trial setting. Pennsylvania law states:

> The proceedings and records of a review committee shall be held in confidence and shall not be subject to discovery or introduction into evidence in any civil action against a professional health care provider arising out of the matters which are the subject of evaluation and review by such a committee.

In addition, committee meeting attendees cannot be compelled to testify in such a civil action and are prohibited from doing so voluntarily.[3] However, these protections are available only if the information is not otherwise available from a non-confidential source.[4] Finally, any individual who provides information to, or who works for a review organization is granted immunity from liability for activities undertaken pursuant to the legitimate review activities of the organization in question.[5] Such individuals must exercise due care, may not be motivated by malice, and the information provided must be related to the review activities and must be true.[6]

Pennsylvania's Peer Review Protection Act has been limited in scope, however, where courts have refused to ap-

---

[Section 5:22]

[1]Rodriguez, "Peer Review Protection Revisited: The Challenge of Transparency with Improvement," *Health Law Handbook*, 246 (A. Gosfield, ed. 2003).

[2]Cal. Evid. Code § 1157(a).

[3]63 P.S. § 425.4.

[4]63 P.S. § 425.4.

[5]63 P.S. § 425.3.

[6]63 P.S. § 425.3.

ply its protections to information gathered by HMOs organized as independent practice associations and the commonwealth Prison Health Services.[7] Conversely, courts in Pennsylvania have applied the protections of the Act to records of the Joint Commission on Accreditation of Hospitals.[8]

§ 5:23 Risk control for provider data: Effective contract drafting—Statutory protections—State Laws—Trade Secrets

Another means of protecting proprietary information is through state trade secret acts. These vary from state to state, but generally they act to protect information that has been kept confidential by an individual or company. The Uniform Trade Secrets Act ("UTSA") defines a "trade secret" as "information, including a formula, pattern, compilation, program, device, method, technique, or process that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[1] The act provides for injunctive relief for actual or threatened misappropriation (which itself includes disclosure without express or implied consent, or acquisition by improper means). Damages may be awarded when misappropriation occurs, which may include both the actual loss and any unjust enrichment caused by the misappropriation. Courts may also award up to double the damages in cases of willful and malicious misappropriation.[2] However, the UTSA contains a statute of limitations of three years—in other words, an injured party must bring suit within three years of discovery (or such point

---

[7]McClellan v. Health Maintenance Organization of Pennsylvania, 546 Pa. 463, 686 A.2d 801 (1996); Joe v. Prison Health Services, Inc., 782 A.2d 24 (Pa. Commw. Ct. 2001).

[8]O'Neill v. McKeesport Hosp., 48 Pa. D & C.3d 115 (Pa. Com. Pls. 1987).

[Section 5:23]

[1]UTSA § 1(4).

[2]UTSA § 3.

where reasonable diligence would have resulted in discovery) of the misappropriation.[3]

The UTSA does not apply to all proprietary data. Obviously, much information that would be of commercial interest is already publicly available (*i.e.*, mortality rates, records of disciplinary action, or even prescription records). In the *Urgent Medical Care* case discussed above, the court found that the information in question (customer lists and demographic information) was proprietary but was not protected by Ohio's Trade Secret Act. The reasoning behind this decision was that, because the information was readily available to the public—even though such information was not necessarily all collected in one location for public use—the information could not be considered "secret." The Ohio Trade Secret Act required that the information not be "published or disseminated, or otherwise become a matter of public knowledge."[4] Under such a definition of "secret," any information collected by a state agency not otherwise kept secret either by the agency or the provider, would fall outside the scope of the definition of a "trade secret." However, other information has the potential to fall within the scope of the UTSA. Examples might include internally developed clinical practice guidelines, patient safety practices, or protocols for delivering care as part of a clinical integration strategy.[5] So long as the provider actually attempts to maintain such information as a secret, and provided the information has economic value when kept as a secret and not available to third parties, a provider should be able to protect its data under the UTSA.

To the extent possible, providers should keep in mind each of the available remedies and control mechanisms mentioned above. Not all protections will apply in all situations, but once a provider has identified what it is they wish to protect, the abovementioned statutes will be important mechanisms in achieving such protection.

---

[3]UTSA § 6.

[4]In re Urgent Medical Care, Inc., 153 B.R. 784, 788 (Bankr. S.D. Ohio 1993).

[5]*See* Leibenluft and Weir, "Clinical Integration: Assessing the Antitrust Issues," *Health Law Handbook*, 13-14 (A. Gosfield, ed. 2004).

§ 5:24 Conclusion

There is an increasingly strong trend towards the disclosure of information in the healthcare industry, especially involving provider quality. In addition, reporting of such information is increasingly required by law. More and more, it is in the provider's best interest to protect and control data that, along with the process for creating the data, is in the provider's control. By doing so, not only will the provider be better able to control such data as it might be used for fodder in a malpractice suit, but also the provider will be more able to exploit the growing commercial value of such data.

Providers will have to remain vigilant in their control and protection of data generated through internal performance measurement activities,[1] outcomes data, clinical practice guidelines and protocols for their implementation,[2] and data prepared for contract negotiations regarding the value of services in terms of cost and outcomes.[3] Heightened sensitivity to protecting how and when data will be used will be a new addition to a provider's checklist for economic risk management in contract drafting in a multiplicity of relationships. Providers must understand the value and need to control their data, as well as the fact that they have mechanisms available to them to achieve this goal.

[Section 5:24]

[1]*See* Gosfield, "The Performance Measures Ball: Too Many Tunes, Too Many Dancers?," *Health Law Handbook*, Ch. 4 (A. Gosfield, ed. 2005).

[2]*See* Gosfield, The Doctor-Patient Relationship as the Business Case for Quality: Doing Well by Doing Right, Journal of Health Law, Vol. 37, No. 12 (Spring 2004).

[3]*See* Leibenluft and Weir, "Clinical Integration: Assessing the Antitrust Issues," *Health Law Handbook*, 20-22 (A. Gosfield, ed. 2004).