

Beyond the Patient: Protection of Registry Data from Litigation and Other Confidentiality Concerns for Providers, Manufacturers, and Health Plans

Draft White Paper for Third Edition of “Registries for Evaluating Patient Outcomes: A User’s Guide”

Background

As the cost of care delivered in the United States continues to grow at an unsustainable rate without parallel improvements in the quality of care,¹ healthcare policy experts and lawmakers are paying increasing attention to initiatives that measure and publicly report information about the performance of physicians, hospitals, and other health care providers as well as the services and procedures that are being delivered. They believe this is an important step to improving health care quality and controlling costs. For example, advancing quality improvement through greater access to and use of health information is a specific goal of the Patient Protection and Affordable Care Act (PPACA),² which includes a number of provisions to incentivize quality measurement, improvement, and reporting as well as enabling more informed decision-making by consumers and other stakeholders.

¹ Fisher, Elliott; Goodman, David; Skinner, Jonathan; Bronner, Kristen; “Health Care Spending, Quality and Outcomes: More Isn’t Always Better,” *Dartmouth Atlas Project Topics Brief* (February 27, 2009). Fisher, Elliott S.; Wennberg, David E.; Stukel, Therese A.; Gottlieb, Daniel J.; Lucas, F.L.; Pinder, Etoile L.; “The Implications of Regional Variations in Medicare Spending. Part 1: The Content, Quality, and Accessibility of Care,” *Annals Internal Medicine*, 138: 273-87 (2003). Fisher, Elliott S., et al.; “The Implications of Regional Variations in Medicare Spending. Part 2: Health Outcomes and Satisfaction with Care,” *Annals of Internal Medicine*. 138: 288-98 (2003). McGlynn, Elizabeth A.; Asch, Steven M.; Adams, John; Keeseey, Joan; Hicks, Jennifer; DeCristofaro, Alison; Kerr, Eve A.; “The Quality of Health Care Delivered to Adults in the United States,” *New England Journal of Medicine*, 348: 2635-45 (2003).

Wennberg, John; Fisher, Elliott, Skinner, Jonathan; “Geography and the Debate Over Medicare Reform,” *Health Affairs Web Exclusive* (February 13, 2002). Wennberg, John E., et al.; “The Dartmouth Atlas of Health Care in the United States 1996,” *American Hospital Publishing, Inc.* (1996). Wennberg, John E.; Brownlee, Shannon; Fisher, Elliot S.; Skinner, Jonathan S.; Weinstein, James N.; “Improving Quality and Curbing Health Care Spending: Opportunities for the Congress and the Obama Administration” *Dartmouth Atlas White Paper* (2008).

de Brantes, François; Rosenthal, Meredith; Painter, Michael; “A Bridge from Fragmentation to Accountability — The Prometheus Payment Model,” *The New England Journal of Medicine*, 361: 1033-1036 (September 10, 2009).

² Patient Protection and Affordable Care Act of 2010 (PPACA), Pub. L. No. 111-148.

Critical to the success of these initiatives is the availability and accessibility of relevant administrative and clinical data. Data registries (or repositories) are often used to collect, process, maintain, and release relevant data for these purposes. For example, many professional associations and societies organized around provider specialties or specific diseases and conditions administer their own registries. Typically, these registries are used for a variety of patient safety and quality improvement activities including: matching patients with researchers, tracking the course of patients' care, tracking and identifying trends with medical errors or other patient safety issues, and tracking outcomes related to specific diseases or conditions or the effectiveness of specific treatments used to treat them. For example, the American College of Chest Physicians (ACCP) directs the ACCP Quality Improvement Registry, Evaluation and Education, or AQUIRE, intended to "assist the chest physician with meeting increasing demands placed upon them by the public, credentialing bodies, regulatory agencies, payers, and the institutions in which they practice."³ Likewise, the American Orthopaedic Association spearheads the Own the Bone registry, designed to better coordinate patient care among a patient's providers, close the gaps associated with physician treatment recommendations, and alter patient and physician behaviors to reduce future incidence of bone fractures due to osteoporosis.⁴ Quality improvement and clinical research registries are also organized by the American College of Rheumatology,⁵ the American College of Radiology,⁶ the Society for Thoracic Surgeons,⁷ and the National Cardiovascular Data Registry.⁸ Similarly, manufacturers and health plans often contribute data to or sponsor registries for quality improvement and clinical research, including identifying care delivery trends and whether or not a particular service, procedure, medical device, or pharmaceutical achieves the desired effect.

Administrative and clinical information submitted by or about providers, medical device and pharmaceutical manufacturers, and health plans and included in registries for research, quality measurement and improvement activities, and patient safety initiatives often includes sensitive patient, provider, and/or manufacturer or health plan-identifiable information. Release of this information in an

³ American College of Chest Physicians. AQUIRE Registry. Available at: <http://www.chestnet.org/accp/quality-improvement/aquire>. Accessed June 23, 2011.

⁴ American Orthopaedic Association. Available at: <http://www.ownthebone.org>. Accessed September 29, 2011.

⁵ American College of Rheumatology. ACR Rheumatology Clinical Registry. Available at: <http://www.rheumatology.org/practice/clinical/rcr.asp>. Accessed June 23, 2011.

⁶ American College of Radiology. National Radiology Data Registry. Available at: <https://nrdr.acr.org/Portal/Nrdr/Main/page.aspx>. Accessed June 23, 2011.

⁷ Society for Thoracic Surgeons National Database. Available at: <http://www.sts.org/national-database>. Accessed June 23, 2011.

⁸ National Cardiovascular Data Registry. Available at: <http://www.ncdr.com/webncdr/common/>. Accessed June 23, 2011.

identifiable or even non-identifiable manner may compromise the privacy of individual patients and providers involved as well as compromise sensitive financial, commercial, or proprietary manufacturer or health plan (e.g., benefit design, reimbursement) information. As more and more registries are developed and used for a variety of research (including comparative effectiveness research), quality improvement, and patient safety programs, the range of information about patient safety, quality of patient care, performance, and other details about providers, medical devices, pharmaceuticals, and health plans grows. This information is incredibly useful to help providers better understand and improve the care they are delivering, help manufacturers refine and improve the devices and pharmaceuticals they are developing, and help patients make more informed choices about their providers and treatment options. However, this information is also desirable for use in litigation or other judicial or administrative proceedings to demonstrate that a certain level of care was adhered to or not or that a certain device or pharmaceutical works in a particular way.

Considerable attention has been directed towards ensuring the privacy and confidentiality of individually identifiable patient health information maintained in registries, particularly in regards to the requirements of The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.⁹ As such, the privacy and confidentiality of individually identifiable patient health information is well established and recognized by Federal and state agencies, courts of laws, and others.

Significantly less attention has been directed towards the privacy and potentially proprietary nature of information supplied by or about providers, medical device and pharmaceutical manufacturers, and health plans. Often providers, manufacturers, and health plans are the best source of information to support the effectiveness of a registry whether it is used for research, quality improvement, patient safety initiatives, or other related activities. Even when they do not directly provide the information to a registry, they may be included in information provided by other sources (e.g., information submitted by a provider relating to a procedure performed on a patient involving Company Y's medical device). Numerous policy makers and researchers have noted the "chilling effect" that the lack of protection for the information provided may have on the willingness of providers, manufacturers, and health plans to provide (or be included as a direct or indirect subject of) relevant information to support research, quality improvement, and patient safety initiatives designed through registries. For example, commentary in the 2006 Journal of the

⁹ 45 C.F.R. pts. 160, 164 (2010).

American Medical Association reported that “wariness about liability exposure in the medical community may stymie public and private efforts.”¹⁰

The 2000 Institute of Medicine (IOM) Report, “To Err is Human”, explicitly identified this “wariness” as a significant issue that hampers voluntary reporting and collaborative efforts, including the free exchange of information, to identify medical errors and prevent their repetition. To address this issue, the IOM report recommended that Congress pass “legislation to extend peer review protections to data related to patient safety and quality improvement that are collected and analyzed by health care organizations for internal use or shared with others solely for purposes of improving safety and quality.”¹¹ To date, however, no comprehensive Federal legislation has been passed. Thus, providers, manufacturers, and health plans must look to a variety of Federal and state laws that may offer protection from disclosure of information pursuant to a discovery request or other judicial or administrative proceedings.

Relevant Laws and Regulations: Variety of Sources, But Limited Protection

While no general Federal statutory privilege exists to protect information held in a registry submitted by or relating to providers, manufacturers, or health plans, there are a number of Federal laws that may provide protection from discovery or disclosure in judicial or administrative proceedings. In addition, most states have specific peer review or quality assurance laws that may provide additional protection as well, but again in limited circumstances. This paper will primarily focus on available Federal evidentiary protections, but will also address state specific protections. It concludes with an overview of mechanisms that may be used to protect information included in a registry during judicial or administrative proceedings and legislative considerations for a new Federal protective model.¹²

¹⁰ Aaron Kesselheim et al. Will Physician-Level Measures of Clinical Performance Be Used in Medical Malpractice Litigation? 295 JAMA 1831 (2006).

¹¹ Institute of Medicine, To Err is Human, 10 (2000).

¹² While registries may collect information from both within the U.S. and internationally, treatment of registries by international laws are outside the scope of this paper.

Federal Laws

AHRQ Confidentiality Statute

All identifiable research data obtained by the Agency for Health Research and Quality (AHRQ) is protected by the agency's confidentiality statute.¹³ The statute requires that data collected by AHRQ-sponsored entities that identifies individuals or establishments be used only for the purposes for which it is supplied. Any effort to determine the identity of a person in an AHRQ database, or to use the information for any purpose other than for research, analysis and aggregate statistical reporting, violates the AHRQ confidentiality statute. Recipients of a data set are also prohibited from releasing, disclosing, publishing, or presenting any individually identifying information. Specifically, the statute provides:

No information, if an establishment or person supplying the information or described in it is identifiable, obtained in the course of activities undertaken or supported under this subchapter may be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented (as determined under regulations of the Director) to its use for such other purpose. Such information may not be published or released in other form if the person who supplied the information or who is described in it is identifiable unless such person has consented (as determined under regulations of the Director) to its publication or release in other form.¹⁴

Concerns have been raised that this protection may be vulnerable if the information is disclosed to an outside entity such as a registry. However, AHRQ has interpreted this provision to protect all AHRQ-funded research from discovery requests, including discovery requests in the course of litigation. A memorandum from senior AHRQ attorney Susan Merewitz noted that "if individuals inside a health care institution are gathering identifiable medical error information as part of AHRQ-supported grant or contract research, and it is conveyed outside the institution, e.g., for analysis in an AHRQ-supported central databank, even if the reporters lost their protection against being subpoenaed to testify under State law, the Federal statute would cover and protect the identifiable information they acquired pursuant to AHRQ's statutory research authority."¹⁵ While this memorandum is not binding on any court of law, and has yet to be introduced in a legal challenge, it clearly establishes AHRQ's protective position as it relates

¹³ 42 U.S.C. § 299c-3(c).

¹⁴ 42 U.S.C. § 299c-3(c).

¹⁵ Memorandum from Susan Merewitz, Senior Attorney, AHRQ, on Statutory Confidentiality Protection of Research Data, to Nancy Foster, Coordinator for Quality Activities. AHRQ. April 16, 2001. Available at: <http://www.ahrq.gov/fund/datamemo.htm>. Accessed September 29, 2011.

to any information collected under the auspices of an AHRQ supported project. Registries participating in AHRQ-sponsored activities would certainly be able to avail themselves of this protection and given the comments of Ms. Merewitz that protection may even extend to non-AHRQ activities where an AHRQ-sponsored entity holds the data as a repository or intermediary.

Importantly, this protection is limited to registries sponsored by AHRQ. Therefore, registries maintained by professional associations or other organizations that are not sponsored by or otherwise participating in an AHRQ-sponsored project would not be able to benefit from the protections afforded by the AHRQ confidentiality statute.

HHS Certificate of Confidentiality

The U.S. Department of Health and Human Services (HHS) may issue a “Certificate of Confidentiality” for any research project that collects personally identifiable, sensitive information and that has been approved by an Institutional Review Board (IRB). A Certificate protects an investigator, and others who have access to research records, to refuse from disclosing identifying information on research participants in any state or Federal judicial, administrative, or legislative proceeding. The Certificate may be used for biomedical, behavioral, clinical or other types of research.

In the research arena, the National Institutes of Health (NIH) is the most common source for Certificates of Confidentiality. The NIH considers research to be sensitive if disclosing the information could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation. According to NIH, examples of studies that may be considered sensitive include those collecting genetic information, information on subjects’ psychological well being, information on sexually transmitted diseases or on subjects’ sexual attitudes, preferences or practices, data on substance abuse or other illegal conduct, and studies where subjects may be involved in litigation related to exposures under study (i.e., breast implants, environmental or occupational exposures).¹⁶

The specific statutory language provides that:

The Secretary [of the U.S. Department of Health and Human Services] may authorize persons engaged in biomedical, behavioral, clinical, or other research (including research on mental health, including research on the use and effect of alcohol and other

¹⁶ See, National Institutes of Health, Certificates of Confidentiality: Background Information, *available at* <http://grants.nih.gov/grants/policy/coc/background.htm> (last visited on Jun. 23, 2010).

psychoactive drugs) to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of such individuals may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals.¹⁷

There are four inherent shortcomings with the applicability of Certificates of Confidentiality to registries.¹⁸ First, the protections only apply to the identity of research subjects, or to data that would allow the possible identification of such individuals. Thus, de-identified patient safety data is still potentially discoverable. Second, there are questions as to whether a Certificate applies to patients who have presumably not consented to becoming research subjects. Third, individual patients may be able to waive the Certificate protections as to their own information, which they presumably would do if they were plaintiffs in a malpractice lawsuit. Fourth, the protections only apply to research information that applies for, and is granted, a Certificate of Confidentiality. Therefore, the protections afforded by a Certificate of Confidentiality are limited and do not provide meaningful opportunities for registries that are not engaged in research and that have not applied for and been granted a Certificate.

The Patient Safety and Quality Improvement Act of 2005

The Patient Safety and Quality Improvement Act of 2005¹⁹ creates a Federal privilege from discovery in connection with Federal or state judicial or administrative proceedings for certain information identified as patient safety work product. To claim the privilege, providers must create the patient safety work product and report it to a formally recognized patient safety organization (PSO) for aggregation and analysis. The term “patient safety work product” encompasses any data, reports, records, memoranda, analyses, or written or oral statements that meet one of two criteria: the materials “could improve patient safety, health care quality, or health care outcomes” and are gathered by a provider to be reported and are reported to a PSO or are developed by a PSO to conduct patient safety activities; or the materials “identify or constitute the deliberations or analysis of, or fact of reporting to, a patient safety evaluation system.”

¹⁷ 42 U.S.C. § 241(d).

¹⁸ Suydam, Steven; Liang, Bryan A.; Anderson, Storm; Weinger, Mathew B.; “Patient Safety Data Sharing and Protection from Legal Discovery,” *Advances in Patient Safety: From Research to Implementation* (Volume 3: Implementation Issues), Published by AHRQ, Feb. 2005.

¹⁹ 42 U.S.C. §§ 299b-21-26.

Materials not gathered to be reported to the PSO and not actually transmitted to a PSO would not qualify for a privilege. The privilege specifically does not apply to medical records, billing and discharge information, or other records kept outside safety reporting systems. Furthermore, providers must comply with any state laws that require reporting of patient safety information. Thus, if a patient safety investigation references medical records, the records themselves do not become part of the work product eligible for protection.

Documents created, maintained, or developed separately from a patient safety evaluation system are excluded from the definition of patient safety work product. Thus, individual patient medical records, billing and discharge information, and any original patient or provider records are not considered work product and are thus not privileged. Indeed, these documents are not work product even if they, or copies of them, are entered into a patient safety evaluation system and/or provided to a PSO. In addition, information collected to comply with external reporting requirements is not work product.

The regulations identify several examples of information that must be reported and does not merit protection as work product, including state incident reporting, adverse drug event information reporting, records for compliance with health oversight agency requirements, reporting physician disciplinary actions to the National Practitioner Data Bank, and disclosures required under Medicare's conditions of participation. Thus, a significant amount of data remains outside the Patient Safety Work Product definition. This includes registry data that is not maintained by a PSO and used for specific patient safety work activities or is not identifiable. Therefore, the PSO statute and regulations provide no protection for registries acting outside the protected scope of the PSO arena.

Quality Improvement Organization Statute and Regulations

Quality Improvement Organizations (QIOs) are responsible for improving the effectiveness, efficiency, economy, and quality of services delivered to Medicare beneficiaries. The Centers for Medicare and Medicaid Services (CMS) contracts with one private, generally not-for-profit organization in every state, as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, to serve as that jurisdiction's QIO. QIO employees, consisting primarily of doctors and other health care professionals, are instructed to review medical care and assist beneficiaries with quality of care issues and complaints, as well as to implement improvements to the quality of care provided by providers.

The QIO statute provides that any data or information acquired by a QIO in its course of duties must be kept confidential and may not be disclosed to any person, except as it assists Federal and state agencies responsible for investigating cases of fraud and abuse, investigating cases involving risks to the public

health, and to assist appropriate state agencies and national accreditation bodies responsible for the licensing or certification of providers or practitioners.²⁰

Furthermore, the statute explicitly states that “no patient record in the possession of” a QIO may be subject to subpoena or discovery proceedings in a civil action.²¹ Additionally, no document or other information produced by a QIO in connection with its deliberations may be subject to subpoena or discovery in any administrative or civil proceeding. However, a QIO shall provide, upon the request of a practitioner or other person adversely affected by such deliberations, a summary of the QIO’s findings and conclusions.

Additionally, QIO regulations state that quality review study information with a patient identifier is not subject to subpoena or discovery in a civil action, including administrative, judicial or arbitration proceedings.²² This restriction, however, does not apply to HHS administrative subpoenas issued in the course of an audit or investigation of HHS programs, in the course of administrative hearings held under the Social Security Act, or to disclosures to the U.S. Government Accountability Office (GAO) as necessary to carry out its statutory responsibilities.

Similar to the PSQIA, the QIO statute and regulations provide protection only to information that has been collected by a QIO under contract with CMS to perform specific statutory functions. To the extent a QIO is the owner and operator of a registry used to perform required functions, the information included in the registry would be protected. However, this does not apply to the vast majority of registries currently in existence today.

HIPAA Privacy Rule

The privacy of individually identifiable health information is protected by the HIPAA Privacy Rule regulations.²³ The Privacy Rule only applies to “covered entities,” which include health plans, health care clearinghouses, health care providers who conduct certain electronic health care transactions, and their business associates (e.g., contractor performing specific functions on their behalf).²⁴ The purpose of the

²⁰ 42 U.S.C. § 1320c-9(b)

²¹ 42 U.S.C. § 1320c-9(d).

²² 42 C.F.R. § 480.140

²³ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 139 (1996) (codified as amended in scattered sections of 42 U.S.C.). HIPAA Privacy Rule Regulations codified at 45 C.F.R. pts. 160 & 164 (2010).

²⁴ 45 C.F.R. § 160.103 (2010).

Rule is to protect all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. “Individually identifiable health information” is information, including demographic data, that relates to an individual’s 1) past, present or future physical or mental health condition; 2) health care provisions; or 3) past, present, or future payment for health care provisions. The information must also identify the individual or reasonably lead to individual identification, and usually consists of common identifiers, such as name, address, birth date, and Social Security Number.²⁵ The Privacy Rule refers to this information as “protected health information” (PHI).

The Privacy Rule includes a liberal exception for disclosure of PHI in the course of any judicial or administrative proceeding in response to an order of a court or administrative tribunal.²⁶ Absent a court order, a covered entity also may respond to a subpoena or discovery request from a party to the proceeding if the covered entity obtains either: 1) satisfactory assurances that reasonable efforts have been made to give the individual whose information has been requested notice of the request; or 2) satisfactory assurances that the party seeking such information has made reasonable efforts to secure a protective order that will guard the confidentiality of the information.

In meeting the first test, a covered entity is considered to have received satisfactory assurances from the party seeking the information if that party demonstrates that it has made a good faith effort (such as by sending a notice to the individual's last known address) to provide written notice to the individual whose information is the subject of the request, that the written notice included sufficient information about the proceeding to permit the individual to raise an objection, and that the time for the individual to raise objections to the court or administrative tribunal has elapsed and no objections were filed or any objections filed by the individual have been resolved.

A “qualified protective order” means an order of a court or of an administrative tribunal or a stipulation that: 1) prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which the records are requested; and 2) requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding. Satisfactory assurances of reasonable efforts to secure a qualified protective order are a statement and documentation that the parties to the dispute have agreed to a protective order and that it has been submitted to the court or administrative tribunal with jurisdiction, or

²⁵ 45 C.F.R. § 160.103 (2010).

²⁶ 45 C.F.R. § 164.512(e).

that the party seeking the protected health information has requested a qualified protective order from such court or tribunal.

Importantly, the protections of HIPAA will only apply if a registry is considered a covered entity or the business associate of a covered entity. This may be the case if the registry is considered a “healthcare clearinghouse” if its function is to “process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements.”²⁷ The more likely scenario is that the registry is acting as the business associate of a covered entity (e.g., collecting and processing information on behalf of provider(s) and/or health plan(s)). However, even if the registry is considered a covered entity or business associate, the minimal protections of HIPAA in the case of disclosure pursuant to a court order, subpoena or discovery request only apply to PHI. To the extent the requested information does not include PHI (e.g., the information is considered to be de-identified), HIPAA does not protect information about providers, manufacturers or any other entities. Therefore, in the case of providers, manufacturers, and health plans seeking protection of de-identified information specific to them or their products, HIPAA does not shield them from discovery requests in litigation or any other court proceedings.

Privacy Act of 1974

The Privacy Act of 1974²⁸ protects information about individuals, such as patients and providers, held by or collected by the Federal government that can be retrieved by personal identifiers such as name, social security number, or other identifying number or symbol. The Privacy Act authorizes a Federal agency to release individually identifiable information to identified persons or to their designees with written consent or pursuant to one of twelve exemptions for disclosure.²⁹ These exemptions include disclosure to Federal agency employees, the Census Bureau, the National Archives and Records Administration, other government entities for civil and criminal law enforcement purposes, the Comptroller General, Congress or its committees, and a consumer reporting agency.³⁰ Additional exemptions include disclosures for statistical research, disclosures required by Freedom of Information Act, disclosures in response to emergency circumstances, and importantly for purposes of this paper, disclosures pursuant to a court order.

²⁷ 45 C.F.R. § 160.103 (2010).

²⁸ Privacy Act of 1974, Pub.L. No. 93-579, § 3, 88 Stat. 1896, 1896 (codified as amended at 5 U.S.C. § 552a (2006)).

²⁹ Privacy Act of 1974, Pub.L. No. 93-579, § 3, 88 Stat. 1896, 1896 (codified as amended at 5 U.S.C. § 552a (2006)).

³⁰ *Id.* at 5 U.S.C. § 552a(b).

Unless the Federal government maintains the registry, the Privacy Act of 1974 offers no protection from discovery for litigation or related court proceedings. Furthermore, even if the Federal government maintains the registry, the Privacy Act specifically allows for the release of identifiable information about individuals without their written consent pursuant to a court order. This could include information not only about individual patients, but also individual providers (e.g., individual practitioners).

Freedom of Information Act

Enacted by Congress in 1966, and expanded in 1996 to cover electronic records,³¹ the United States Freedom of Information Act (FOIA)³² generally provides that any person has the right to obtain access to information contained in the records of Federal agencies, unless such information is specifically protected from disclosure by FOIA. With a goal of ensuring an informed citizenry, capable of holding the government accountable, FOIA effectively establishes a statutory right of public access to executive branch information, requiring that virtually every record held by a Federal agency be provided to individuals upon request.³³ Information that is subject to FOIA is likely to be disclosable pursuant to a discovery request or other court proceeding. However, FOIA does have limited exemptions and exclusions to the broad disclosure requirements. The most relevant exemptions for purposes of protection of registry information are Exemption Four, Exemption Six, and Exemption Three.

Exemption Four protects “trade secrets and commercial or financial information obtained from a person and privileged or confidential.”³⁴ Importantly, however, it is not a mandatory bar to disclosure, but rather limits an agency’s obligation to disclose specified information. “Trade secrets” are defined as commercially valuable plans or formulas for producing trade commodities to which has been invested substantial effort or innovation.³⁵ In the case of registries that contain information supplied by or about providers, medical device or pharmaceutical manufacturers, and health plans, it is likely that only the pharmaceutical and medical device manufacturers and health plans would have information that could be considered “trade secrets.” Furthermore, information contributed to a registry by manufacturers is more likely to be considered “commercial” or “financial.” For example, in Public Citizen Health Research

³¹ Electronic Freedom of Information Amendment Acts of 1996, Pub. L. No. 104-231, 110 Stat. 3048 (1996) (codified as amended at 5 U.S.C. § 552).

³² Freedom of Information Act, 5 U.S.C. § 552 (2006), *amended by* OPEN Government Act of 2007, Pub. L. No. 117-175.

³³ U.S. Department of Justice. Freedom of Information Act Guide (2004). Available at: http://www.justice.gov/oip/introduc.htm#N_2. Accessed September 29, 2011.

³⁴ 5 U.S.C. § 552(b)(4).

³⁵ 45 C.F.R. § 5.65(a).

Group v. Food & Drug Administration,³⁶ the court found that “because documentation of the health and safety experience of their products will be instrumental in gaining market approval for their products it seems clear that the manufacturers ... have a commercial interest in the requested information.”³⁷

Exemption 6 states that information about individuals in "personnel and medical files and similar files" can be withheld from disclosure by Federal agencies when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy."³⁸ In order to warrant protection under Exemption 6, the information at issue must first meet the threshold requirement of falling into one of three categories – personnel files, medical files and similar files. The Supreme Court found that Congress intended these categories to be interpreted broadly and to protect information that “applies to a particular individual.”³⁹ Once it has been established that the information meets this threshold, the focus shifts to whether the disclosure of such information would be an unwarranted invasion of privacy. This requires balancing the public’s right to disclosure of the information against the individual’s right to privacy. After determining that a protectable privacy interest exists, the public’s interest in disclosure of the information will be weighed against the individual’s privacy interest in not disclosing the information.

The landmark Supreme Court decision in *United States Department of Justice v. Reporters Committee for Freedom of the Press*⁴⁰ governs how privacy interests under Exemption 6 are determined and balanced with public interest in the information. First, the Court clarified that a substantial privacy interest may exist in information that has already been released to the public at some point. Second, the Court held that the identity of the individual or party requesting the information may not be taken into consideration when determining if information should be released and “has no bearing on the merits of his or her FOIA request.”⁴¹ When considering the public interest in disclosing the information, the Court ruled that the determination should be based on the nature of the requested information and its relationship to the public interest generally, and not solely the purpose for which the request is made. Finally, the Court narrowed the scope of the public interest to the kind of interest to information that will “shed light on an agency’s performance of its statutory duties.”⁴²

³⁶ Pub. Citizen Health Research Group v. Food & Drug Admin., 704 F.2d 1280 (D.C. Cir. 1983).

³⁷ 704 F.2d at 1290.

³⁸ 5 U.S.C. § 552(b)(6).

³⁹ See U.S. Dep’t of State v. Washington Post Co., 456 U.S. 595, 602 (1982).

⁴⁰ U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).

⁴¹ 489 U.S. at 771.

⁴² 489 U.S. at 773.

It is important to note, however, Exemption Six only protects information that identifies the individual in question. Thus, while patient records included in a registry are likely to be protected, if identifying information is removed, the information is no longer protected under Exemption Six. The most common types of information protected under Exemption Six are age, home address, Social Security number, medical information about individuals participating in clinical research trials, claims files, and other personal information held by CMS.⁴³

Exemption Three protects information if it is “specifically exempted from disclosure by statute, provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.”⁴⁴ An example of a statute that may prevent disclosure or discovery of information contained in a registry under FOIA Exemption Three would be the Patient Safety Quality Improvement Act of 2005 (discussed above) if the information met the PSQIA requirements.

Federal Trade Secrets Act

The Federal Trade Secrets Act⁴⁵ imposes fines or imprisonment on any Federal employee who discloses any information that relates to trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses or expenditures of any person or corporation. The Act applies only to public disclosures, and does not reach internal agency use of the data.

There is no private right of action under the statute; however, the Administrative Procedure Act may create a right of action to prevent a violation of the Trade Secrets Act or review a decision to disclose information.⁴⁶ Similar to Exemption Four under FOIA, the Federal Trade Secrets Act may protect proprietary information, however, only to the extent that is held by the Federal government and disclosed publicly (e.g., may not reach information disclosed pursuant to a protection order as part of a discovery proceeding.).

Federal Rules of Evidence and Civil Procedure

Federal legal rules of evidence and civil procedure may place limits on what information may be discoverable or otherwise used in a court proceeding. For example, Rule 401 of the Federal Rules of

⁴³ 45 C.F.R. § 5.67(c).

⁴⁴ 5 U.S.C. § 552(b)(3).

⁴⁵ 18 U.S.C. § 1905.

⁴⁶ 76 C.J.S. *Records* §111 (2011).

Evidence defines “relevant evidence” as evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.”⁴⁷ Rule 403 narrows the scope of Rule 401 stating “although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury...”⁴⁸ Often of the most relevance to information contained in registries is the bar in Rule 404 against “evidence of other ... acts ... to prove the character of a person in order to show action in conformity therewith.”⁴⁹ This may apply in instances where information is sought from a registry to show evidence of similar medical outcomes.

Turning to Civil Procedure, Rule 26(b)(2)(C)(iii) of the Federal Rules of Civil Procedure provides that a court may limit discovery if “the burden or expense of the proposed discovery outweighs its likely benefit, considering ... the importance of the discovery in resolving the issues.”⁵⁰ Rule 26(c) also allows parties from whom discovery is sought to move for a protective order.⁵¹ Rule 45(c) protects individuals from unduly burdensome or expensive subpoenas. Specifically, 45(c) states, “a party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The issuing court must enforce this duty and impose an appropriate sanction — which may include lost earnings and reasonable attorney's fees — on a party or attorney who fails to comply.”⁵² It is left to the discretion of the court in each case to determine whether the facts and circumstances merit quashing a specific subpoena.

While these Federal rules of evidence and civil procedure may offer protection against discovery of registry information in certain situations, their application is left entirely to the discretion of the particular court in which the case is heard. Thus, the case law is mixed with some courts allowing discovery and others not depending on their application of a balancing test of the need for confidentiality vs. hardship to the party seeking discovery. For example, in *Andrews v. Eli Lilly & Co., Inc., E.R. Squibb & Sons and Rexall Drug Company*,⁵³ Squibb sought production of data from a University of Chicago registry that included information about a disease related to a products liability action against Squibb. The University of Chicago claimed that the contents of the registry were privileged and confidential. In balancing the

⁴⁷ Fed. R. Evid. 401.

⁴⁸ Fed. R. Evid. 403.

⁴⁹ Fed. R. Evid. 404(b).

⁵⁰ Fed. R. Civ. P. 26(b)(2)(C)(iii).

⁵¹ Fed. R. Civ. P. 26(c).

⁵² Fed. R. Civ. P. 45(c).

⁵³ *Andrews v. Eli Lilly & Co., Inc.*, 97 F.R.D. 494 (1983).

privacy interests of the registry against the need for the information, the court stated, “the balance ... tips in favor” of the registry.⁵⁴ “Squibb’s need for the information is speculative and uncertain. Its essentially private interest in defending itself is outweighed by the compelling social interest in preventing harm to the Registry and the vital work it conducts.”⁵⁵ The court, however, did allow discovery of information contained in the registry related to the plaintiffs. Squibb appealed and in *Deitchman v. E.R. Squibb & Sons*,⁵⁶ the appellate court noted that the privilege was not “absolute” and remanded the case back to the lower court to determine the best way to provide information from the registry while preserving confidentiality.⁵⁷ In a second hand smoke case, *Wolpin v. Phillip Morris Inc.*,⁵⁸ the court ordered disclosure of data from a statewide tumor registry from a study by the University of South California and California Department of Health despite objections that the data was protected by state and Federal privacy laws. The court held that the confidentiality interest was outweighed by the need for the information in the lawsuit, but did require patient names to be removed prior to release.

[Patient Protection and Affordable Care Act: Release of Medicare Claims Data for Provider Performance Measurement and Reporting](#)

Section 10332 of PPACA requires the Secretary to make Medicare claims data available to qualified entities for the evaluation of provider performance on measures of quality, efficiency, effectiveness, and resource use.⁵⁹ The data are standardized extracts of claims data under parts A, B, and D for items and services furnished for one or more specified geographic areas and time periods requested by a qualified entity. The qualified entities will be required to pay a fee to obtain the data and must submit to the Secretary of HHS a description of the methodologies that will be used to evaluate the performance of providers and suppliers.

All subsequent reports published by a qualifying entity must include an understandable description of the measures, risk adjustment methods, physician attribution methods, other applicable methods, data specifications and limitations, and the sponsors, so that consumers, providers of services and suppliers, health plans, researchers, and other stakeholders can assess such reports. In addition, the reports must be made available to any provider or supplier identified in the report, with an opportunity to appeal and

⁵⁴ 97 F.R.D. at 502.

⁵⁵ 97 F.R.D. at 502.

⁵⁶ *Deitchman v. E.R. Squibb & Sons, Inc.*, 740 F.2d 556 (7th Cir. 1984).

⁵⁷ 740 F.2d at 561.

⁵⁸ *Wolpin v. Phillip Morris, Inc.*, 189 F.R.D. 418 (C.D. Cal. 1999).

⁵⁹ Patient Protection and Affordable Care Act, Pub. L. 111-148, § 10332 (2010).

correct any errors. Finally, the reports may only include information on a provider or supplier in an aggregate form as determined appropriate by the Secretary.

The Secretary may not make claims data available to a qualified entity unless the entity agrees to release the information on the evaluation of performance of providers of services and suppliers. Section 10332 requires that data released to a qualified entity shall not be subject to discovery or admission as evidence in judicial or administrative proceedings without consent of the applicable provider or supplier.⁶⁰

While limited in application to Medicare claims data provided to qualified entities, this provision is a significant recognition by Congress of concerns related to the “chilling effect” the fear of disclosure has on provider, supplier (including manufacturer), and health plan participation in quality measurement, improvement and reporting programs. By shielding this information from discovery or admission as evidence without consent, Congress has explicitly protected and incentivized the activities of qualified entities, including the development of registries to support their performance measurement and reporting efforts.

State Laws

State Surveillance Laws

To encourage practitioner participation in state surveillance registries, many states have passed legislation providing immunity from civil and criminal penalties that may arise in conjunction with such reports. Most states protect providers from any liability that may result from a disease report unless the provider acted with some level of negligence or malicious intent.⁶¹ Fewer states provide complete immunity for reporting disease cases to a registry, with no distinction made for negligent or intentionally malicious reports.⁶² Additionally, other states provide immunity only for certain causes of action related to the information reported, or protect from civil liability only.⁶³ However, case law implicating such state

⁶⁰ Patient Protection and Affordable Care Act, Pub. L. 111-148, § 10332(e)(4)(D) (2010).

⁶¹ *See, e.g.* VA. CODE ANN. § 32.1-38 (2011) (immunity from civil liability or criminal penalty unless such person acted with “gross negligence or malicious intent”); ARIZ. REV. STAT. ANN. § 36-666 (2010) (immunity from civil or criminal liability if the provider acted in “good faith and without malice”); IOWA CODE § 139A.3 (2010) (immunity from any liability, civil or criminal, for any person “acting reasonably and in good faith” while reporting); KAN. STAT. ANN. § 65-118 (2010) (immunity from any liability, civil or criminal, if provider reported “in good faith and without malice”).

⁶² *See, e.g.* N.C. GEN. STAT. § 130A-142 (2010) (a provider who reports “shall be immune from any civil or criminal liability that might otherwise be incurred or imposed as a result of making that report”).

⁶³ *See, e.g.* NEB. REV. STAT. § 71-503.01 (2010) (immunity for providers from suits for slander, libel, or breach of privileged communication); NEV. REV. STAT. § 629.069 (2010) (immunity for providers from civil liability only).

harbors is sparse, with most cases affording immunity for health care professionals who report sexually transmitted diseases discovered in minors in potential child abuse cases.⁶⁴

State Peer Review and Quality Assurance Laws

Presently, all 50 states have enacted statutes to protect the confidentiality of the peer review process. Most statutes offer a blanket protection for all accounts, records and conclusions of the review process from being introduced into evidence during any court proceeding.⁶⁵ Without such protection, providers and hospitals may be less inclined to truthfully monitor their peers, evaluate the quality of care that is provided to patients, or to adequately prevent or correct for adverse events.

A few states also have passed legislation specifically protecting information collected for quality improvement and other related purposes. These “safe harbor” laws protect a broader set of information beyond the traditional peer review process, including collection by organizations outside the scope of an internal peer review board or committee. For example, in Minnesota, information relating to patient care collected by a nonprofit organization for purposes of “evaluating and improving the quality of health care” or “reviewing the safety, quality or cost of health care services” provided to health plan enrollees “shall not be disclosed to anyone . . . and shall not be subject to subpoena or discovery.”⁶⁶ The Virginia Patient Safety Act protects the collection of patient safety data by “statewide or local associations” representing licensed health care providers. It treats the information collected as “privileged communications which may not be disclosed or obtained by legal discovery proceedings unless a circuit court, after a hearing and for good cause arising from extraordinary circumstances being shown, orders the disclosure of such proceedings, minutes, records, reports, or communications.”⁶⁷ Similarly the Illinois Medical Studies Act protects all information “used in the course of internal quality control or of medical study for the purpose of reducing morbidity or mortality, or for improving patient care or increasing organ and tissue donation.” Such information is “privileged, strictly confidential, and shall be used only for

⁶⁴ See, e.g. *KB v. Mills*, 639 N.W.2d 261 (Mich. Ct. App. 2002); *State v. Superior Court*, 930 P.2d 488 (Ariz. Ct. App. 1997); *Alicia T. v. Cnty of L.A.*, 222 Cal App. 3d 869 (Cal. Ct. App. 1990); *Criswell v. Brentwood Hospital*, 551 N.E.2d 1315 (Ohio Ct. App. 1989).

⁶⁵ See e.g., Idaho Code § 39-1392 (2011) (“all peer review records shall be confidential and privileged, and shall not be directly or indirectly subject to subpoena or discovery proceedings or be admitted as evidence, nor shall testimony relating thereto be admitted in evidence, or in any action of any kind in any court or before any administrative body, agency or person for any purpose whatsoever”); Ohio Rev. Code Ann. § 2305.252 (2011) (“proceedings and records within the scope of a peer review committee of a health care entity shall be held in confidence and shall not be subject to discovery or introduction in evidence in any civil action against a health care entity or health care provider. . .).

⁶⁶ Minn. Code § 154.61 (a, g), § 145.64 (2010).

⁶⁷ VA. CODE ANN. § 8.01-581.17 (2011)

medical research, increasing organ and tissue donation, [or] the evaluation and improvement of quality care.”⁶⁸ It is not “admissible as evidence, nor discoverable in any action of any kind in any court or before any tribunal, board, agency or person.”⁶⁹

However, it is important to note that the peer review privilege and other state-based protections are often not recognized in Federal cases outside the jurisdiction of state law. Federal courts have been resistant to establish a Federal peer review or other privilege, and often subordinate the state peer review privileges in favor of other interests. For instance, the 11th Circuit Court of Appeals recently declined to recognize such a privilege during a Federal civil rights discrimination case, ordering the discovery of peer review documents.⁷⁰ Similar outcomes have been reached in many other Federal courts, including cases deciding Federal antitrust⁷¹ and wrongful termination claims.⁷²

Practical Considerations

As described above, Federal and state law currently do not provide any consistent or comprehensive protection from disclosure pursuant to discovery or other judicial or administrative proceedings of information submitted by (or that is related to) providers, medical device or pharmaceutical manufacturers, or health plans to registries. This leaves registries that are operating outside of the government-sponsored programs described above, their participants and subjects, vulnerable to discovery requests ranging from preliminary fact-finding requests to court orders. As the IOM noted this can have a “chilling effect” on willingness of providers to participate. The same is also true for manufacturers and health plans that similarly may be both a source of information as well as the subject of information included in a registry. Beyond concern for the privacy and confidentiality of the information, the costs and burden associated with discovery or other requests can be substantial often taking months or years as the litigation process unfolds. These costs may include not only costs related to challenging the request, but also data production, including costs for redaction (particularly where patient identifiable information is involved), and the costs of legal representation.

There are several steps that registries as well as their participants can take to reduce their vulnerability to disclosure requests. As described above, there are several Federal programs that protect information

⁶⁸ 735 Ill. Comp. Stat. 5/8-2101 (2010).

⁶⁹ 735 Ill. Comp. Stat. 5/8-2012 (2010).

⁷⁰ *Adkins v. Christie*, 488 F.3d 1324 (11th Cir. 2007).

⁷¹ *Marshall v. Spectrum Medical Group*, 198 F.R.D. 1 (D. Me. 2000).

⁷² *Price v. Howard County Gen. Hosps.*, 950 F. Supp. 141 (D. Md. 1996).

collected for specific patient safety and quality improvement purposes. If registries qualify for or are funded through these programs, the information collected and maintained would automatically be entitled to protection from discovery or other judicial or administrative proceedings. While not always possible or practical given their goals or priorities, registries should consider whether or not participation in any of these programs would be appropriate.

To the extent participation in one of these Federal programs is not possible, registries and their participants should consider formation in a state that provides broader protection for information collected beyond the peer review process (e.g., VA, MN, or IL). Furthermore, registries and their participants should clearly articulate their roles and responsibilities, including how discovery or other requests will be handled. Registries should develop specific policies and procedures that will guide their response to any such requests and should ensure that all participants are familiar with the policies and procedures. For example, registries might stipulate that they will direct all disclosure requests to the original source of the information where possible. Where information held within a registry has been aggregated and analyzed such that it is significantly modified from its original state, the registry will notify the original data sources prior to compliance with any discovery request and give them the opportunity to object.

In the event a registry is compelled to release information pursuant to a court order or other judicial or administrative order, registries may request certain information be redacted or a protective order issued. A court protective order can stipulate who can see the information, who has access to the information, and rules for destruction or return of the data. Similarly, a registry may request that the information be “sealed” by the court so that they are not made public. These types of actions have historically been used to protect patient-identifiable information held in registries, however, they may be similarly applied to confidential or proprietary information related to providers, manufacturers or health plans.

Conclusion

As more and more attention is focused to the development and implementation of quality improvement activities, including those tied to new payment models, availability and accessibility of underlying clinical and administrative data that registries can provide to support these efforts will be increasingly important. This emphasis will be further strengthened as the new Patient Centered Outcomes Research Institute authorized to support efforts to generate comparative effectiveness research begins its work. Given this heightened interest in registries as a data source, the issue of protection of registry data from disclosure pursuant to a discovery request or other judicial or administrative proceedings will be increasingly

important. Registry sponsors may be able to address concerns from potential participants about data protection by considering these issues during the registry development stage. In particular, providers, manufacturers, and health plans that are developing a registry or considering participation in a registry should look to the variety of Federal and state laws described here that may offer protection and should consider the practical steps outlined above to reduce their vulnerability to disclosure requests.