P•C•R•C

PHYSICIAN CLINICAL REGISTRY COALITION

GUIDANCE ON LEGAL CHALLENGES AND REGULATORY OBLIGATIONS FOR CLINICAL DATA REGISTRIES

FEBRUARY 2015

American Academy of Dermatology Association ◆ American Academy of Neurology ◆ American Academy of Ophthalmology ◆ American Academy of Physical Medicine and Rehabilitation ◆ American Association of Neurological Surgeons ◆ American College of Emergency Physicians ◆ American College of Surgeons ◆ American Gastroenterological Association ◆ American Joint Replacement Registry ◆ American Society for Radiation Oncology ◆ American Society of Clinical Oncology ◆ American Society of Nuclear Cardiology ◆ American Society of Plastic Surgeons ◆ American Urological Association ◆ Anesthesia Quality Institute/American Society of Anesthesiologists ◆ GIQuIC/ American College of Gastroenterology ◆ National Association of Spine Specialists ◆ Society for Vascular Surgery ◆ Society of Interventional Radiology ◆ Society of Neurointerventional Surgery ◆ The Society of Thoracic Surgeons

PHYSICIAN CLINICAL REGISTRY COALITION MEMBERS

American Academy of Dermatology Association

American Academy of Neurology

American Academy of Ophthalmology

American Academy of Physical Medicine and Rehabilitation

American Association of Neurological Surgeons

American College of Emergency Physicians

American College of Surgeons

American Gastroenterological Association

American Joint Replacement Registry

American Society for Radiation Oncology

American Society of Clinical Oncology

American Society of Nuclear Cardiology

American Society of Plastic Surgeons

American Urological Association

Anesthesia Quality Institute/American Society of Anesthesiologists

GIQuIC/ American College of Gastroenterology

National Association of Spine Specialists

Society for Vascular Surgery

Society of Interventional Radiology

Society of Neurointerventional Surgery

The Society of Thoracic Surgeons

Disclaimer:

This Guidance document is provided for informational and educational purposes only. It is not intended to provide and should not be treated as legal advice. Registries should consult with their own counsel in making determinations about legal and regulatory issues affecting their operations.

For further information:

This Guidance was prepared for the Coalition by its legal counsel, Powers Pyles Sutter & Verville PC. Questions about the document can be addressed to Rob Portman at rob.portman@ppsv.com. Samantha Marshall, Amita Sanghvi, and Sarah Imhoff also made substantial contributions to the drafting of this Guidance.

Table of Contents

EXECUTIVE SUMMARY

Clinical data registries or repositories ("Registries") collect and analyze data on treatment outcomes submitted by physicians, hospitals and other types of health care providers related to a wide variety of medical procedures, diagnostic tests, and/or clinical conditions. Registries are often sponsored by national medical societies or their affiliates, universities, health insurers, or other entities. Their primary purpose is to produce benchmarks or metrics that their participating health care providers ("Participants") can use to improve the quality of care they provide their patients. Registries also engage in research projects to enhance general knowledge about the safety and effectiveness of various medical procedures, diagnostic tests, treatments, and health care products. Other registries, such as public health databases, collect data on various population health events that may or may not involve medical treatment.

The federal government, health care products manufacturers, and state and local governments have increasingly come to rely on Registries for a wide variety of purposes. For instance, the Food and Drug Administration ("FDA") has been encouraging drug and device manufacturers to work with Registries to conduct investigational and post-approval surveillance studies to ensure that both unapproved and approved drugs and devices are safe and effective. The Centers for Medicare & Medicaid Services ("CMS") has required participation in Registries as a condition of reimbursement for certain medical procedures that involve investigational or off-label (i.e., unapproved) uses of drugs or devices. Similarly, the Centers for Disease Control and Prevention ("CDC") and state and local governments are relying on other kinds of data registries to track public health crises and responses.

At a time when the need for Registries is growing, so too are the legal challenges and regulatory burdens. Registries are subject to overlapping and duplicative federal rules governing the privacy and security of their data. They incur potential liability risk to patients, manufacturers, and others when they publish data and issue reports evaluating the efficacy of medical procedures or health care products. Registry data are also potentially subject to burdensome and costly legal discovery or subpoenas that threaten to drain Registry resources and discourage participation by health care providers.

The Physician Clinical Registry Coalition ("the Coalition") is a group of more than twenty medical society-sponsored or physician-led Registries working for public policies to facilitate Registry development and to remove unnecessary legal and regulatory burdens on their operations. The Coalition is providing this Guidance to assist Registries in their understanding of several of these legal and regulatory challenges. This Guidance analyzes (i) the federal and state privacy issues facing Registries; (ii) ownership of Registry data; (iii) FDA medical device reporting requirements; (iv) liability risks associated with publishing benchmarks, analyses, or research studies on particular medical procedures, diagnostic tests, drugs, or devices using Registry data; and (v) available protections from legal discovery of Registry data under federal and state law.

We have focused on federal law in this Guidance. We cover state law more generally, but Registries should identify the specific rules

EXECUTIVE SUMMARY

that apply to their operations in each state from which they collect or in which they maintain their data or a substantial business presence.

The guidance provided in this paper can be summarized as follows:

I. **Privacy Issues**—Registries must comply with the regulations issued under the Health Information Portability and Accountability Act of 1996 ("HIPAA")[1] and the Common Rule,[2] to the extent applicable, if they collect identifiable patient information from their Participants. The requirements of the HIPAA regulations and the Common Rule are complicated and overlapping. The Coalition is advocating for policy changes that would lessen these duplicative regulatory burdens without diminishing patient protection. Registries must also comply with state privacy laws, particularly in the states where the Registry has offices or holds data. Registries must adopt appropriate policies and procedures and purchase cyber security insurance to protect against the risk of data breaches and other privacy violations.

II. **Data Ownership**—Ownership of Registry data is determined by state law and therefore varies based on the location of the Registry. Typically, Participants (not patients) own the medical records they create from patient encounters. Patients may or may not own the data in their medical records, but, in any case, they have a well-established right or interest in most states to review or seek modifications in their records. Registries own their aggregated data and databases. These distinctions need to be clearly articulated in Registry agreements with Participants ("Participation Agreements"). Registries should also understand and plan for the possibility that other stakeholders may also have (or at least claim) an ownership interest in Registry data. These stakeholders may include health insurers, government agencies, or device or drug manufacturers if they fund Registry data collection activities or contribute data to the Registry.

III. **FDA Device Reporting**—FDA medical device reporting rules do not affect Registries directly, but Registries may need or wish to assist Participants and device manufacturers in meeting their obligations under these rules.

IV. **Liability Risks—**Registries face liability risks in publishing their data or data analyses. Registries may have liability to Participants or patients if they publish erroneous data or data reports on the efficacy of certain procedures or health care products, and patients are harmed as a result. They may also have liability risk to drug or device manufacturers if they publish negative reports about the performance of particular health care products. Registries can best manage this risk by ensuring that the data and data reports they publish are current and accurate. Registries that are affiliated with national medical societies or other similar membership or multistakeholder organizations would also risk violating the antitrust laws if they were to use Registry data or reports to limit the ability of particular health care products companies or health care providers to compete in their particular markets.

V. **Legal Discovery—**A fundamental concern in creating and operating a Registry is the risk that the information submitted to the

EXECUTIVE SUMMARY

Registry by providers and manufacturers will be subject to legal discovery—for example, through a subpoena issued by a plaintiff in a malpractice action against a provider or a products liability suit against a device manufacturer or through a discovery request in direct litigation against a Registry. There is no general federal statutory protection against the discovery of Registry data in legal proceedings. The Federal Rules of Civil Procedure provide some protection against requests for Registry data, particularly in precluding disclosure of patient identifiable information. These rules may or may not protect against the disclosure of provider data, depending on the circumstances. The Patient Safety Organization ("PSO") Act[3] and implementing rules[4] do provide some protection against legal discovery, but that protection is subject to judicial interpretation and limitation; not all Registries can qualify as a PSO; and the PSO rules add significant regulatory burdens, potential penalties for noncompliance, and the risk of forfeiture of data if a Registry ceases to be a PSO. Many states have peer review and other laws that would protect against the discovery of Registry data in most circumstances, but these laws generally would not apply in a federal case based on federal law. The Coalition is advocating for broad federal legislation that would protect Registry data from legal discovery, whether through third-party subpoenas or direct litigation against Registries.

Guidance on Legal Challenges and Regulatory Obligations for Clinical Data Registries

The Coalition is providing this Guidance to assist Registries in their understanding of several legal and regulatory challenges that affect their ability to collect, protect, and analyze clinical data. The issues covered include: (i) the federal and state privacy issues facing Registries; (ii) ownership of Registry data; (iii) FDA medical device reporting requirements; (iii) liability risks associated with publishing benchmarks, analyses, or research studies on particular medical procedures, diagnostic tests, drugs, or devices using Registry data; and (iv) available protections from legal discovery of Registry data under federal and state law.

We focus on federal law, but Registries must also understand the state laws that affect their operations. This Guidance does not address all of the legal issues that Registries face; rather it focuses on those that are not only important, but also tend to raise policy issues that affect a Registry's prospects for success, many of which the Coalition is trying to address through its advocacy efforts.

I. Privacy Issues

The Health Information Portability and Accountability Act of 1996 ("HIPAA")[5] and its implementing regulations are the primary federal law affecting the privacy of patient data collected by Registries. Most states also have their own laws that protect identifiable patient data. For the most part, Registries are safe in establishing procedures and processes for protecting their data that comply with HIPAA regulations. However, Registries should adopt strategies for complying with state data protection laws where they are more stringent than the HIPAA regulations.

a. HIPAA

The rules issued under HIPAA establish a federal regulatory framework for the use and disclosure of protected health information ("PHI") by health care providers and other entities with which they share PHI. Specifically, the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") has issued both Privacy and Security Rules (collectively, the "HIPAA Rules") to implement the statute.[6]

PHI is individually identifiable health information that requires patient authorization for use and disclosure unless such disclosure falls within one of many exceptions.[7] HIPAA applies to "covered entities," defined to include health care providers that transmit health information in electronic form, health plans, and health care clearinghouses, as well as "business associates," defined as entities that provide services for or perform functions on behalf of covered entities. [8]

The enactment of the American Recovery and Reinvestment Act ("ARRA") in 2009 extended HIPAA requirements and penalties to business associates.[9] Among other things, these changes subject business associates to the same penalties for unauthorized disclosure as covered entities and require business associates to notify individuals (or covered entities) and, in certain instances, the Secretary of Health and Human Services ("the Secretary"), in the event of a breach.[10] Business associates must also have appropriate policies and procedures to comply with the requirements of the Privacy and Security Rules.

The Privacy Rule allows for the disclosure of PHI by a covered entity without patient authorization for the purposes of treatment, payment, or health care operations.[11] Health care operations include, among other activities, quality assessment and improvement activities.[12] The Privacy Rule requires either a patient's authorization or a waiver of such authorization from an institutional review board ("IRB") or privacy board if PHI is being disclosed for research purposes.[13] "Research" means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.[14]

The extent to which HIPAA applies to the activities of a Registry will depend on the nature of the data being collected, the purpose of the collection, and whether that Registry is actually physically receiving the data. For example, a Registry would not be subject to HIPAA limitations when handling de-identified information, which is information that contains no personal identifiers or unique identifying numbers, characteristics, or codes.[15] Similarly, if a Registry collected "limited data sets," it would not need to obtain patient authorization or a waiver of such authorization from an IRB. [16] A limited data set is information that is partially de-identified by removing direct identifiers like name, address, phone number, and email address; but that retains certain PHI, such as an individual's gender, date of birth, or address containing only the city, state, or zip code.[17] The limited data set exception applies only to the use of data for research, health care operations, and certain public health purposes. This exception requires the covered entity to enter into a data use agreement with the limited data set recipient to preserve the confidentiality of the data and restrict its use. The Privacy Rule establishes specific requirements for such agreements.

The HIPAA Rules permit covered entities to share PHI with business associates for treatment, payment, or health care operations purposes if they enter into business associate agreements that meet regulatory requirements for protecting PHI. [18] Covered entities may only disclose to business associates the "minimum necessary" information for the business associate to perform its services or functions.[19]

Registries typically act as business associates of their participating physicians and hospitals, which are almost always covered entities under the HIPAA Rules. Registries usually perform data aggregation and related benchmarking analyses that support Participants' quality improvement efforts and other health operations. As such, Registries need to have a business associate agreement in place with each Participant prior to receiving the Participant's PHI.[20] If a Registry is subcontracting with a data management vendor for the collection, hosting, and/or analysis of Participants' PHI, a Registry must also have a sub-business associate agreement in place with the vendor. The same would be true for any other subcontractors with which the Registry wishes to share PHI.

Under the HIPAA Rules, the Registry's business associate status allows it to receive and analyze each site's data and report back aggregate results to all of its sites; but it cannot share the PHI of any one Participant with other Participants, except with the permission of all of the Participants whose data is being shared.[21] No patient authorization is necessary for Participants to send PHI to a Registry if the Registry has a HIPAA-compliant business associate agreement in place with each Participant and the disclosure is for health care operations and not research purposes.

The OCR has also indicated that no patient authorization is necessary if a Registry collects

data from Participants primarily for quality improvement/health care operations purposes, and then de-identifies the data and uses that for later research activities.[22] However, if a Registry wishes to ***disclose*** PHI to a third party for research purposes, a business associate agreement will not be sufficient to meet the HIPAA requirements for such disclosures, even if the primary purpose of collecting the data was for health care operations. Instead a Registry would need to obtain individual authorization or an IRB waiver of authorization for the disclosure of PHI,[23] as well as consent from the relevant Participants. For some types of research, it may be impracticable for researchers to obtain written authorization from individuals. For example, if a Registry is collecting retrospective data from Participants, it may be impossible and/or unduly burdensome to track down patients and get them to sign HIPAA authorizations. In such cases, Registries would need to seek an IRB waiver of the patient authorization requirement.

IRB waivers of the HIPAA patient authorization requirement are granted if the following conditions are met:[24]

1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
    a. an adequate plan to protect the identifiers from improper use/ disclosure;
    b. an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining identifiers or such retention is otherwise required by law; and
    c. adequate written assurances that PHI will not be reused/disclosed to any other person or entity, with certain exceptions.
2. The research could not practicably be conducted without an alteration or waiver.
3. The research could not practicably be conducted without access to and use of the PHI.

Registries collecting retrospective data can usually persuade an IRB to grant a waiver of authorization on grounds that it is impracticable and unduly expensive to obtain authorizations from the patients.

Importantly, OCR permits and encourages central IRB waivers of authorization—*i.e.*, waivers from a single IRB that apply to several covered entities participating in clinical trials or similar activities, including submitting data to Registries, and does not require the Participants to obtain separate waivers from their local IRBs.[25] Of course, Participants may still insist on obtaining local IRB approval and waivers to comply with their institutional policies.

The HIPAA Rules also permit a covered entity to disclose PHI to a public health authority [26] for certain public health activities and purposes, including ". . . preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions. . . .."[27] Thus, where a state or federal law authorizes a public health authority to collect certain public health-related PHI, for example, immunization data, a covered entity may share this information with a Registry operated by or on behalf of the public health authority without an individual's consent. The HIPAA Rules do not specify what types of procedures a public health authority must take to protect the privacy and security of PHI it receives under the public health exception. Public health-related registries would be well-advised to follow the same rules that apply to covered entities and business associates for the protection of PHI.

b. Common Rule

The Federal Policy for the Protection of Human Subjects or the "Common Rule" is codified in separate regulations by fifteen Federal departments and agencies, most of which are located in the Department of Health and Human Services ("HHS"). The Common Rule outlines the basic provisions for IRBs, informed consent, and "Assurances of Compliance" by institutions covered by the Common Rule. Human subject research conducted or supported by each federal department/agency is governed by the regulations of that department/agency.[28]

The Common Rule applies to research that is "conducted, supported or otherwise subject to regulation by any federal department or agency which takes appropriate administrative action to make the policy applicable to such research."[29] In other words, the Common Rule applies to federally-funded research and research that is conducted pursuant to federal regulations. The Common Rule defines "research subject to regulation" as:

> [R]esearch activities for which a federal department or agency has specific responsibility for regulating as a research activity, (for example, Investigational New Drug requirements administered by the Food and Drug Administration). It does not include research activities which are incidentally regulated by a federal department or agency solely as part of the department's or agency's broader responsibility to regulate certain types of activities whether research or non-research in nature (for example, Wage and Hour requirements administered by the Department of Labor).[30]

Where the Common Rule applies, it covers research involving human subjects, which includes the collection of identifiable patient information.[31] The Common Rule generally does not apply to privately-funded research activities not otherwise subject to federal regulation.[32] Most Registries do not receive federal funding or conduct studies subject to federal regulation, and therefore are not subject to the Common Rule. However, many hospital Participants, particularly academic medical centers, are subject to the Common Rule because they receive federal research grants and other federal funding and/or participate in clinical trials regulated by the National Institutes of Health ("NIH") or the FDA. Even if a particular research project is not federally funded or otherwise subject to federal regulation, many academic medical centers have signed "federalwide assurances" that require them to follow the Common Rule for any research they conduct.[33]

The Office for Human Research Protections ("OHRP"), the agency that administers the Common Rule for HHS, has clearly stated that entities that collect data in the course of clinical care and submit that data to external researchers are not engaged in human subjects research and therefore are not subject to the Common Rule with respect to such activities, even if they have signed federalwide assurances. Specifically, OHRP has issued guidance stating that "[i]nstitutions whose employees or agents release to investigators at another institution identifiable private information or identifiable biological specimens pertaining to the subjects of the research" are not engaged in human subjects research.[34] OHRP has further indicated that this guidance applies to hospitals, physician groups, and other covered entities that are otherwise covered by the Common Rule, but are only submitting data to Registries in the normal course of treating patients, and are not performing research themselves on that data.[35] This conclusion applies even if the covered entity is contacting the patient for information on how the patient's condition is progressing, as long as such follow-

up activities are part of the normal treatment protocol.

In short, the Common Rule does not apply to hospitals and physician groups submitting data to Registries for health care operations or research purposes if they are simply submitting data to Registries collected in the normal course of clinical care and are not involved in the research themselves.

Even where the Common Rule does apply to entities that submit data to Registries, OHRP has clearly stated that data sources can rely on IRB waivers of the Common Rule consent requirements obtained by sponsors of clinical trials or other researchers, such as Registries.[36]

The Common Rule generally requires covered researchers to obtain informed consent from patients to participate in human subjects research and to implement safeguards for protecting the privacy and security of identifiable patient data collected for such efforts. Researchers are required to obtain informed consent or an IRB waiver of such consent, even if they are only collecting patient data from health care providers and not conducting clinical trials or otherwise interacting directly with patients. The Common Rule requirements for protecting patient data are generally less stringent than, but nonetheless duplicative of, the parallel requirements under the HIPAA Rules. To avoid these redundant regulatory burdens, the Coalition has asked OHRP to create an exception to the Common Rule for entities that are only collecting identifiable patient data (*i.e.*, and not interacting directly with patients) and that are in compliance with the relevant HIPAA Rules for protecting the privacy and security of patient data. OHRP is still considering this request.

c. State Privacy and Breach Notification Statutes

The HIPAA Rules only preempt any state laws that provide less protection for patient privacy.[37] Many states have privacy and breach notification laws that impose more stringent privacy and security protections related to the use or disclosure of patient medical information.

For instance, California has a breach notification law that applies to licensed health facilities, clinics, home care agencies, and hospices in California.[38] The law requires these covered entities to report a breach of medical information to the California Department of Public Health and to affected individuals within five business days after a breach "has been detected." By contrast, the HIPAA Rules require covered entities and business associates to report a breach of unsecured PHI within sixty calendar days of determining that such breach has occurred.[39] California law does not define "detected." For instance, it is not clear whether the clock starts ticking on the five-business-day reporting obligation only when the covered institution learns of the breach or when one of its subcontractors, like a Registry, learns of the breach. Because of this uncertainty, it is common for California Participants to take a conservative approach and require its Registry partners to report any breach of PHI to the Participant within no more than five business days, and often less.

Access to medical records is another example of where state laws may be more stringent than HIPAA. In Virginia, a health care entity is required to provide patients access to their records with fifteen days of receiving a request.[40] By contrast, the HIPAA Rules require health care entities to provide this access within thirty days of a request.[41] Although the Virginia

law does not apply directly to Registries, a Virginia Participant may request that a Registry provide the Participant access to medical records managed by the Registry within the shorter time frame.

Compliance with states laws poses significant challenges for Registries that collect data from hospitals and/or physicians in many states. Registries should work with participating hospitals and physician groups in each state to identify local privacy and security rules that may be more stringent than the HIPAA Rules and that may require changes in a Registry's normal procedures for protecting patient data or reporting unauthorized uses or disclosures.[42]

d. State Common Law

Beyond federal and state privacy statutes, many states recognize a general, common law right to privacy and will hold entities and individuals legally responsible for violation of that right. The common law right of privacy will hold an individual liable for interfering with another's right to privacy by publicly disclosing personal facts.[43] Thus, the Registries should be aware that not only are they subject to state breach notification requirements, but they may also be liable for the negligent disclosure of PHI through state common law privacy claims. Most likely, these claims would arise in the form of demands for indemnification from a Participant that is sued for a Registry's wrongful disclosure of PHI. Likewise, such claims could also be brought against a Registry if the Participant has wrongfully submitted PHI to the Registry. Accordingly, most Registry participation and business associate agreements include mutual indemnification provisions identifying the circumstances under which Registries and their Participants will indemnify each other for wrongful acts or omissions that give rise to third-party liability claims.

As business associates covered by HIPAA and other privacy laws, Registries that have access to or control over PHI collected from Participants must have HIPAA-compliant policies and procedures in place before they start collecting data. They may also need policies to comply with the Common Rule and state privacy laws to the extent applicable to their activities. In addition, Registries should purchase sufficient cyber security insurance to protect against the risk of data breaches or other HIPAA/privacy violations.

II. Data Ownership

Data ownership is determined by state law, either in the state where the data originated, where the data is held, or where the Registry's principal offices are located. The law in most states gives health care providers ownership over the medical records they keep from patient encounters. Patients have rights of access to or modification of their records to correct errors, but they may or may not own the data gathered by their health care provider.

Registries, by contrast, can and should own the compilation of data that they collect from Participants. This means Registries should own the aggregate data they create from Participants' raw data submissions, as well as the databases in which Participant's data is kept.

To avoid any doubt or controversies, Participation Agreements should clearly spell out these legal distinctions and state that (i) the Participant owns the raw data it submits (subject to any rights of patients), (ii) the Participant has the authority to submit the data to the Registry, (iii) the Registry owns its aggregate data and database(s), and (iv) the Registry is not required to return the data to the Participant upon termination or expiration of the Participation Agreement. The Participation

Agreement should also state that the Registry will continue to protect the Participant's data under HIPAA and other applicable laws as long as the Registry continues to possess the data.

Other Registry stakeholders may have or claim an ownership interest in Registry data. For instance, a manufacturer that funds the development of a data module within the Registry or a study of the effectiveness of the company's drug or device may claim that it owns the data in the module or the study data. The Registries' agreements with these other funders or data sources should clearly define who owns the data contributed or funded.

Registries should also consider whether to register their database, data reports, or other original works of authorship with the U.S. Copyright Office. The Registry's database would typically be subject to federal copyright protection as a compilation, provided that there is some originality to the development of the database.[44] The underlying data itself normally would not be covered by the copyright laws. Although registration is not required for copyright protection, a copyright holder can only sue for infringement under federal law and receive statutory damages after a work has been registered. However, Registry databases should have protection and the right to sue under state/common law copyright laws even if they do not register with the Copyright Office.

III. FDA Medical Device Reporting

The FDA requires medical device manufacturers, importers, and user facilities to report medical device adverse events they become aware of to the FDA to address problems in a timely fashion.[45] A medical device distributor is defined as any person who "furthers the marketing of a device" but who "does not otherwise repackage or otherwise change the container, wrapper or labeling of the device or device package."[46] Distributors must maintain records of reportable incidents but need not actually report them.[47]

A device user facility includes "a hospital, ambulatory surgical facility, nursing home, outpatient diagnostic facility, or outpatient treatment facility" but does not include school nurse offices or employee health units.[48] Device user facilities are required to report "deaths and serious injuries that a device has or may have caused or contributed to" to both the FDA and the manufacturer.[49] These facilities are also required to submit summary annual reports to the FDA and maintain adverse event files.[50]

Manufacturers are defined as persons (1) who actually make a device; (2) who otherwise repackage the container, packaging, or labeling of a device; or (3) who have another party make a device according to the manufacturer's specifications.[51] Manufacturers must submit reports of adverse events to the FDA within thirty calendar days of learning of the event. These adverse events include those that cause death or serious injury or malfunctions that if repeated could cause death or serious injury. Manufacturers also must report any event that "requires remedial action that presents unreasonable risk of substantial harm" or those for which the FDA requested a report be made within five working days of learning of the event. Manufacturers may also need to submit supplemental reports as necessary.[52]

Registries do not qualify as any of the entity types covered by the FDA medical device reporting requirements and therefore are not obligated to report adverse events to the FDA but could decide to do so voluntarily.[53] Registry Participants, however, may qualify as "user facilities" and must adhere to the Medical Device Reporting ("MDR") requirements.[54] If a Registry shares data with manufacturers on the performance of their devices, including data that suggests a device may have caused serious injuries to patients, that information could

obligate the manufacturer to report to the FDA.[55] Therefore, Registries may need to include provisions in their Participation Agreements with Participants or their data sharing agreements with manufacturers to address the Participants' or manufacturers' MDR requirements.

IV. Liability Risks for Procedure or Product Evaluations

A Registry could face liability risk based on its evaluation of the effectiveness of certain procedures, drugs or devices, or other health care products, and publish the results. This liability risk could arise if a Registry conducts its own studies or if it conducts studies on behalf of manufacturers. For instance, some Registries conduct FDA-regulated post-market surveillance, investigational device exemption ("IDE"), or investigational new drug ("IND") studies for manufacturers.

In theory, a Registry could be liable to patients if it published reports or studies finding that a particular procedure, drug, or device was effective when in fact it was later found to be ineffective or harmful. We are not aware of any case law in which such a claim has been brought against a Registry.[56] Registries generally would not be required to warn patients of product safety or effectiveness problems. However, if a Registry is publishing benchmarks on the performance of particular health care providers or health care products, it is possible that a court could find that the Registry has a duty of care in developing and disseminating those benchmarks. This would be similar to the duty of organizations that set standards or test consumer products.[57]

Likewise, if a Registry is conducting a study on behalf of a manufacturer, it could be treated as an extension of that manufacturer for liability purposes. It should, therefore, make sure that its study agreements with manufacturers include appropriate indemnification provisions, liability releases, and other protections against third–party claims.

More generally, Registries that make a claim about the safety or effectiveness of a medical procedure, drug, or device based on Registry data should continue to update that claim based on additional or new data to avoid a possible lawsuit should a manufacturer, physician, or patient rely on it.

A Registry also could face liability risk if it publishes a negative evaluation of a manufacturer's product, and the manufacturer sues that Registry under a trade disparagement, antitrust, or similar legal theory.[58] Trade disparagement claims are based in state law and would allow a manufacturer of a drug or device to sue a Registry for making an allegedly false claim about the efficacy or safety of a particular drug or device when a Registry allegedly knew that the statement was false. Under federal law, a manufacturer could also bring a claim concerning false statements, misleading descriptions, or false or misleading representations of fact about a device under the Lanham Act, the United States trademark law, for devices that are protected under a trademark.[59]

Registries, as with other entities, generally cannot be held liable on a trade disparagement theory simply for making negative statements about a manufacturer's product. For example, an insurer's statement that a manufacturer's device had "no proven clinical utility . . . since it [was] considered to be investigational," without any evidence that the person or organization making the statement knew it to be false, was not enough to establish an insurer's liability to a device manufacturer on a trade disparagement theory.[60] Internal documentation that the insurer did in fact believe the device had no proven clinical use was useful in defending

against the trade disparagement claim in that case.[61]

In another case brought under both the Lanham Act and a state common law disparagement theory, the same manufacturer sued the American Association of Electrodiagnostic Medicine ("AAEM")[62] over a literature review published in AAEM's peer-reviewed journal that evaluated the manufacturer's device. The literature review concluded that the evidence of the utility of the company's medical device was inconclusive. The court held that AAEM was not liable in part because for a challenge to be brought under the Lanham Act, the speech at issue must be "commercial," that is, related to a commercial transaction or the speaker's economic interests.[63] Because the AAEM article only considered the usefulness of the device at issue and did not evaluate anything commercial in nature, the article did not violate the Lanham Act prohibition against disparaging speech. The court also noted that to "chill" the AAEM's statements in this case would prevent "all debate about such subjects from entering the marketplace."[64] So long as a Registry is not making statements or claims based on Registry data that are commercial in nature, it is unlikely to be held liable under the Lanham Act.

As to the state level disparagement or injurious falsehood claims, the court held that there was no liability under Maryland law for these claims where the statements were made without malice.[65] Whether malice is required for all state law disparagement claims or whether knowledge that the statements were false is sufficient to impose liability will vary from state to state. Registries and the organizations that support them therefore should be careful about making any statements about a drug or device that cannot be supported by objective scientific facts and data. They should also update any conclusions drawn on Registry data if a Registry becomes aware that the statements are no longer accurate.

For Registries that are sponsored by medical societies—and therefore are considered to be a combination of competitors—product evaluations can also lead to antitrust claims if a manufacturer alleges that a Registry disparaged one of the manufacturer's devices or drugs to limit competition or to prevent the device from being purchased in the relevant market. Of course, if a manufacturer can show that a medical society engaged in *intentional* conduct to harm the competitive position of a particular manufacturer or group of manufacturers— e.g., by sharing data with some manufacturers and not others— the risk of antitrust liability would increase dramatically.[66]

Because of the risks of these lawsuits, if a Registry does decide to evaluate specific drugs or devices, it should make sure it has insurance that covers this activity. As noted above, if a manufacturer affirmatively asks or seeks to engage a Registry to evaluate the company's product and publish its results, the Registry should insist that the manufacturer provide written indemnification provisions and liability releases for the Registry's evaluation activities. The Registry should also ensure that any public statements that it makes about particular drugs or devices are accurate and not misleading. In addition, entities that create Registries might consider setting up a separately-incorporated subsidiary to house the Registry and thereby limit the parent organization's liability risk. Generally, separate incorporation will prevent third parties from attacking the parent corporation's assets based on actions of the subsidiary. The parent organization should weigh the cost and administrative burden of establishing and operating the Registry as a separate entity against the liability protection offered by separate incorporation.

V. Data Protection Issues

A fundamental concern in creating and operating a Registry is the risk that the

information submitted to the registry by providers and manufacturers will be subject to legal discovery—for example, through a third-party subpoena[67] issued by a plaintiff in a malpractice action against a provider or a products liability suit against a device manufacturer or through a discovery request in direct litigation against a Registry. This section discusses the potential federal and state laws that might protect a Registry data from legal discovery and concludes there is a need for general federal legislation to protect Registries against discovery of identifiable Registry data.

a. Federal Rules of Civil Procedure

Rule 45 of the Federal Rules of Civil Procedure ("FRCP") applies to subpoenas issued in federal cases against third parties.[68] FRCP 45(d)(1) contains the provisions for protecting recipients of subpoenas from undue burden and expense. Attorneys issuing subpoenas have an affirmative obligation to avoid imposing such burdens, and courts are directed to enforce this duty and impose sanctions against a party or attorney who violates this prescription.

FRCP 45(d)(2)(B) allows a person who receives a third-party subpoena to file objections "to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested." In the face of such objections, the person issuing the subpoena is then required to withdraw or modify its request or file a motion to compel production.

FRCO 45(d)(3) provides several grounds under which a reviewing court may quash or modify a subpoena, including if the subpoena requests disclosure of privileged or other protected matter (if no exception or waiver applies), or subjects a person to undue burden. The court is permitted, but not required, to quash or modify a subpoena that asks for disclosure of a trade secret or confidential research, development, or commercial information. In making these assessments, courts typically will review some or all of the requested information in camera (*i.e.*, in private chambers), balance the competing interests, and then render a decision.[69]

For cases in which a Registry is a party to a lawsuit, the Registry would rely on FRCP 26(c) to protect its data from discovery requests. Discovery can take the form of requests for documents or data, oral or written depositions, or interrogatories for a Registry that can be addressed by a Registry as a whole.[70] FRCP 26(c) allows a court, "for good cause," to "issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." This includes "forbidding the disclosure or discovery" or using other means to limit the discovery, including limiting it by time and place, prescribing other discovery methods that may be less invasive, limiting the scope of disclosure, or prohibiting or limiting how a trade secret or confidential research is revealed.[71] While FRCP 45(d) offers some protection to Registries concerning requests for information when they are not a party to a lawsuit, FRCP 26(c) offers comparable protections to the Registry once it becomes a party to a lawsuit.

In practice, federal courts have typically been very reluctant to disclose identifying information of patients or trade secrets of manufacturers unless the patient or company is a party to the suit. Instead, they will usually only permit discovery of aggregated, non-identifiable data, unless a compelling case is made for disclosing identifying information.[72] In some instances, the court will find that the sensitive nature of the information itself merits preservation of registry participants' privacy and confidentiality.[73] Courts also are reluctant to admit evidence of

other bad acts to prove the liability of a defendant in a particular case arising out of a particular set of circumstances.[74] If a Registry were to receive a subpoena or discovery request seeking aggregated data, it could still object on grounds of undue burden or expense or lack of relevance of the data, but courts would be much less sympathetic to such arguments unless a significant actual burden could be demonstrated.

Two of the leading federal cases illustrating these principles are *Farnsworth v. Proctor & Gamble* and *Deitchman v. E.R. Squibb & Sons, Inc.*, both products liability cases in which manufacturers sought data from a registry.

In *Farnsworth vs. Proctor & Gamble*, P&G sought the names and addresses of women participating in a CDC study on Toxic Shock Syndrome ("TSS") in an effort to discredit the study findings.[75] The plaintiffs sought to recover damages from P&G for TSS allegedly caused by "Rely" tampons manufactured by the company. Responding to P&G's third-party subpoena, the CDC turned over virtually all of the documents relating to its study, except the names and addresses of the study subjects. It did turn over the names and addresses of patients who consented to have their information disclosed to P&G. Relying on FRCP 26(c) (even though this case involved a third-party subpoena), the *Farnsworth* court upheld the district court's order that the privacy interests of the study participants outweighed the discovery interests of the manufacturer and denied disclosure of the patient names and addresses.

In *Deitchman v. E.R. Squibb & Sons, Inc.,* the court applied a similar balancing test in deciding whether to disclose patient registry records maintained by the University of Chicago ("U of C").[76] The suit was filed against Squibb and other drug companies seeking compensation for injuries allegedly caused by *in utero* exposure to the drug diethylstilbestrol ("DES"). As part of discovery, Squibb had asked the court to issue subpoenas for literally every document in U of C's cancer registry. The U of C registry was the only central repository of data on the relationship between DES and clear cell adenocarcinoma of the genital tract, the principal disease at issue in *Deitchman.* The data in the registry were the primary basis for studies on the effect of DES in causing this form of cancer that were being used against Squibb in the case.

U of C filed a motion to quash under FRCP 45 (b), claiming its data were privileged and confidential. Here, the court acknowledged the need to protect the privacy of registry participants' information, and indeed assumed for the sake of argument that the data were protected by a qualified privilege. But, the court also gave significant weight to Squibb's need to defend itself and the importance of having access to the data on which studies showing the relationship between DES and genital tract cancer were based. As a result, the court held that the manufacturer was entitled to some limited discovery of registry data, while protecting the patients' confidentiality and the interests of the registry. The court did not fashion a discovery order itself, but instructed the district court to do so in a way that would not require disclosure of patient identifying information and would otherwise protect patient confidentiality through the potential use of impartial third parties to review and report on the data. It concluded by stating, that the district court should work with the parties to develop an order that "allows Squibb the least necessary amount of information to avoid a miscarriage of justice without doing needless harm to . . . [a] Registry."[77]

Other courts considering subpoenas of Registry data have similarly sought to balance the public interest in allowing the disclosure of necessary information for purposes of litigation or to expose research to critical inquiry and the need to protect the identity of study and Registry Participants. For example, a California District Court allowed production of raw data from a study on lung cancer in women exposed to secondhand smoke using data from a state-sponsored cancer registry so long as the identities of the individuals in the study who had not authorized the release of the data were kept confidential. In doing so, the court upheld a magistrate judge's decision to compel disclosure subject to certain confidentiality protections.[78]

Farnsworth, *Deitchman,* and other case law show that federal courts will look at all the facts and circumstances in determining whether to allow the discovery of Registry data. But, for the most part, courts are very unlikely to permit disclosure of patient identifying information. It is less clear whether the courts will permit data on specific providers or products to be disclosed. *Farnsworth* and *Deitchman* involved requests by manufacturers for data on their products. So they shed no light on how federal courts would resolve a discovery request by a plaintiff's attorney for Registry data on a specific manufacturer's product. But we do know the courts would balance the manufacturer's proprietary interests in preserving trade secrets and other confidential information against the discovering party's need for the data in the litigation.

We are not aware of any federal cases involving discovery requests for Registry data on a specific hospital's or physician's outcomes. However, as noted above, such requests might be denied on grounds that such data would not be relevant to prove poor performance in a particular case. Plus, if a Registry were providing regular reports to a hospital or physician on their quality outcomes, the plaintiff could obtain the reports from the defendant hospital or physician.

b. HIPAA

HIPAA regulations, while providing stringent confidentiality and security measures, have a relatively liberal exception for the disclosure of PHI in judicial and administrative proceedings. The exception allows for the disclosure of PHI in response to a court order or pursuant to subpoena, discovery request, or other lawful process so long as the covered entity receives "satisfactory assurance" that reasonable efforts have been made to give notice to the affected party or to obtain a protective order.[79] Given this broad, relatively accessible exception, it is fair to say that HIPAA provides no greater protection for the Registry data against a discovery request than would be generally available under the FRCP 26(c) or 45. Indeed, the HIPAA Rules actually provide less protection because they only safeguard PHI, not provider or manufacturer information.[80]

c. Patient Safety Organizations

The formation of a Patient Safety Organization ("PSO") may provide a Registry with additional protections against discovery but also creates several new regulatory burdens and risks, including the risk of losing Registry information should the PSO status be revoked or relinquished. The Patient Safety Organization Act ("PSOA") protects against the legal discovery of identifiable patient safety work product ("PSWP") collected by a PSO.[81] This includes protection against federal, state, or local civil, criminal, or administrative subpoenas or discovery and protection against this work product being admitted as evidence in the same proceedings or admitted or accessible as part of a disciplinary proceeding against a provider,

subject to certain exceptions.[82] In order to obtain this protection, a Registry would have to qualify as and meet the ongoing requirements of a PSO and Registry data would have to constitute identifiable PSWP,[83] which is by no means a given. This protection is limited to identifiable data and is not self-enforcing.[84] Thus, a PSO could have to go to court to enforce the PSO discovery prohibition.

The downsides to forming a PSO, among other things, are that the Registry would be subject to government audits and potential sanctions for non-compliance with PSO rules.[85] The PSO confidentiality rules also significantly limit the ability of PSO Participants to make public statements about their performance in relation to benchmarks established by a PSO Registry because such information would be based on PSWP submitted by the Participants.[86] Most importantly, a Registry that voluntarily decides not to maintain its PSO status or is disqualified for noncompliance with the PSO rules would have to transfer its PSWP to another PSO, return the data to its source, or destroy the data.[87]

Importantly, the PSO privilege language is not self-enforcing—that is, the assertion of the privilege can be challenged in court—and is therefore subject to judicial interpretation and limitation. To date, PSOs attempting to protect information from discovery collected pursuant to state incident reporting requirements have had little success in court. In the 2014 case *Tibbs v. Bunnell*, the Supreme Court of Kentucky ruled that state-mandated incident reports held by a PSO are not privileged under the PSOA because the plain language of the Act does not protect "information collected, maintained, or developed separately, or existing separately from a patient safety evaluation system."[88] Because Kentucky law mandates that "incident investigation reports" be "*established, maintained and utilized* as necessary to guide the operation of [a] facility" and that facilities must have policies and procedures for recording such incidents,[89] the court held that they had been created separately from the system protected by the PSOA. The court further held that this information could be discovered only after an "in camera" review by the court to separate discoverable information from information that was privileged.[90]

In a second 2014 case, *Charles v. Southern Baptist Hospital of Florida*, a Florida Circuit Court similarly found that information held by a PSO that was collected "pursuant to a healthcare provider's obligation to comply with federal, state, or local laws, or accrediting or licensing requirements [was] not privileged" under the PSOA, based on the same statutory language cited in *Tibbs*.[91] The *Charles* court held that this limitation applies to any information that is merely "collected" or "maintained" to comply with "external obligations" and not just information actually provided to the government.[92] Thus, in Florida, information collected under state record keeping requirements that can be reviewed on request by the state Agency for Health Care Administration is not privileged under the PSOA.[93] The holdings in both *Tibbs* and *Charles* are limited to their respective state jurisdictions. As of the date of this Guidance, the *Charles* case was being appealed to the Florida appeals court.

Thus, while PSO status provides the most direct federal protection of Registry data from legal discovery, the protection comes with significant regulatory risks and burdens, it is not self-enforcing, and it may be limited by judicial interpretation. Each Registry must balance the risks and limitations of the PSO discovery protections against the benefits.

d. AHRQ Protections

The Agency for Healthcare Research and Quality ("AHRQ") may offer some protection for Registry data against legal discovery. This protection would be available only if a Registry received AHRQ funding or received data from an entity that has received AHRQ funding related to a Registry's data.

AHRQ's confidentiality statute, 42 U.S.C. § 299c-3(c), limits the use of information compiled in an AHRQ-sponsored study to the original purpose for which the information was supplied unless the person or establishment supplying the information has consented to its use for other purposes. AHRQ has broadly interpreted this provision to protect data against all forms of legal discovery and has concluded that such protection travels with the data, and therefore is not limited to the data of entities directly receiving funding. In addition, AHRQ has pledged to assist recipients of AHRQ funding in convincing courts to adopt AHRQ's broad interpretation of § 299c-3 (c).[94]

It is important to note that AHRQ's position on its ability to protect AHRQ-funded data has not been tested in a court of law and the protections that it offers become weaker the more removed an entity is from the actual recipient of AHRQ funding. In another AHRQ-sponsored memorandum, the authors noted that the confidentiality protections offered through the AHRQ statute may become more attenuated where the AHRQ-sponsored organization is merely operating as a "repository" for patient safety data collected by a non-AHRQ sponsored entity and is not collecting the data itself.[95] Moreover, the language of § 299c-3(c) does not explicitly protect data from legal discovery. Without an explicit legislative protection, there is no guarantee that information provided to an AHRQ-funded Registry would be protected from disclosure.[96] Additionally, as with PSOs, becoming a recipient or sub-recipient of AHRQ funding, or even just affiliating with such an entity, could result in the loss of at least some control over the data and subject the Registry to substantial additional federal regulatory requirements that apply to recipients of federal funding.

e. Certificates of Confidentiality

The NIH issues Certificates of Confidentiality to protect investigators and institutions from legal discovery of information that could be used to identify subjects within a research project.[97] Specifically, the authorizing statute covers "[p]ersons so authorized to protect the privacy of [research subjects from being] compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals,"[98] a statement that is confirmed by the NIH in its guidance documents.[99] Certificates of Confidentiality are issued to institutions or universities where the research is conducted and, according to the NIH, afford permanent protection to research subjects that participate in research projects covered by these certificates, even to those patients who may have submitted research data to the institution before the certificate was issued.[100] Certificates of Confidentiality only protect patient information, not providers or institutions.

Certificates of Confidentiality generally apply only to specific research projects, not to broad classes of research or data collection, such as would be the case for a Registry. They also only apply to certain types of sensitive research. NIH defines sensitive to mean "that disclosure of identifying information could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation."[101] Examples of such research include collecting "genetic information," "information on psychological well-being," s exual information, and information "on substance

abuse or other illegal risk behaviors." It also includes "studies where subjects may be involved in litigation related to exposures under study."[102] Given their narrow scope and applicability, it is unlikely that a Registry, or the research projects it sponsors or facilitates, would qualify for a Certificate of Confidentiality.

f. State Law

The lack of comprehensive federal statutory protection for Registry data from legal discovery suggests that a Registry may need to look to state law for protection, at least to fight subpoenas issued in state court proceedings or federal cases that involve state law claims. As a general rule, a plaintiff in a lawsuit filed in state court ***outside*** the state in which a Registry is located would have to ask a state court ***within*** the Registry's home state to issue a third-party subpoena seeking Registry data. The court reviewing the subpoena would most likely apply its own state law rather than the law of the state in which the lawsuit was filed.

The general standards in most states for evaluating such subpoenas are similar to those set forth in the FRCP 26(c) and 45. However, some states have special statutes that would provide additional protection for Registry data if a Registry can show these laws apply to a particular subpoena.[103] Of course, these state statutory protections would not necessarily apply if the underlying lawsuit were filed in federal court and solely involved federal law claims, in which case FRCP 26(c) or 45 would likely govern.

A review of all of the potential state statutes that might protect Registry data is beyond the scope of this document. Registries should focus their review of state data protection laws in the state in which the bulk of Registry data collection activity takes place, the state where the data is stored, and the state in which the Registry or sponsoring organization is incorporated. These are the most likely places where a subpoena would have to be issued to obtain Registry data, and, therefore, the most likely jurisdictions whose data protection laws would be applied.

g. Limited Research Privilege

There may also be some cases where a Federal court, relying on state law, will accord a "qualified privilege" to scholarly research to protect the public interest in promoting this research as part of the balancing test for admitting evidence applied under Rule 201 of the Federal Rules of Evidence.[104] State courts might also grant this qualified privilege under analogous state rules of evidence. Where available, this privilege could be used to protect research data beyond the confidentiality of patient information. For example, in *Dow Chemical Co. v. Allen*, the court barred discovery pursuant to an administrative subpoena of all working papers, notes, reports, and raw data of an unfinished animal toxicity study in part on the grounds that the risks of premature disclosure to the development of the research outweighed the value of the data to the litigation.[106] While the data in *Dow* received protection, this protection would not necessarily have extended to separate litigation that depended more heavily on the animal toxicity study data. The case indicates, however, that there may be some circumstances in which a court will exclude data from consideration in a case or investigation to protect the integrity of the research itself.

In addition, in *Cusumano v. Microsoft Corporation*, the court, applying FRCP 45, also denied production of two academicians' research materials on the grounds that academicians are entitled to the same pre-publication privilege as journalists, subject to a balancing of the interests in disclosure against the interests in protection of the information.[106] In reaching this conclusion, the court cited case law from other federal appellate courts holding

that the medium by which an individual engages in investigative reporting does not change the amount of protection that the work receives.[107] It may also be possible to assert this privilege in state court, either through a balancing of interests, as in *Dow Chemical,* or by the assertion of a specific state law research privilege.[108] In addition to the protections that may be available for patient data, Registries with pre-publication data that are designated for a specific research purpose may be able to gain additional protections for this data pending publication.

In sum, other than those provided under the PSO laws, there are no specific federal statutory privilege protections for Registry data. The federal evidentiary rules do provide some protection for such data, particularly identifiable patient data. HIPAA provides some protection for PHI legal discovery, but it provides no protection for provider or manufacturer data. While the PSO Act contains a federal privilege for identifiable PSWP, the costs/risks of becoming a PSO must be balanced against the benefits of the statutory privilege. The affiliation with a recipient of AHRQ funding may enhance the protection of Registry data, but could also create additional burdens and result in the possible loss of control of the data. Certificates of Confidentiality do protect against legal discovery, but most Registry research would likely not qualify for such a certificate.

Registry data likely will receive some privilege protections under state law, but Registries must review the laws in the states where they do business or are conducting their Registry activities to determine whether there are laws in place that would protect their data from discovery. In addition, in some rare cases a qualified privilege for pre-publication data may be available to Registries. But these state law protections may not always be available in federal court proceedings.

Based on this lack of clear federal protection of Registry data from legal discovery, the Coalition is working on developing federal legislative proposals that would provide such protection without the onerous conditions imposed by the PSO Act and rules.

Additional Resources

For additional resources on registry legal and policy issues, please see the following:

Agency for Healthcare Research and Quality, United States Dept. of Health and Human Servs., Pub. No. 13(14)-EHC111, Registries for Evaluating Patient Outcomes: A User's Guide (Richard E. Gliklich et al. eds., 3rd Ed. 2014), *available at* http://effectivehealthcare.ahrq.gov/index.cfm/search-for-guides-reviews-and-reports/?productid=1897&pageaction=displayproduct

United States Gov't Accountability Office, Clinical Data Registries: HHS Could Improve Medicare Quality and Efficiency through Key Requirements and Oversight, Pub. No. GAO-14-75 (Dec. 2013), *available at* http://www.gao.gov/assets/660/659701.pdf

End Notes

1. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified at 42 U.S.C. § 1320d *et seq.*).
2. *See* United States Dep't of Health and Human Servs*., Federal Policy for the Protection of Human Subjects ('Common Rule')*, http://www.hhs.gov/ohrp/humansubjects/commonrule/index.html (last visited January 15, 2015).
3. Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. §§ 299b-2, 299b-26 (2014).
4. 42 C.F.R. Part 3 (2014).
5. 42 U.S.C. § 1320d *et seq.* (2014).
6. 45 C.F.R. pts. 160 and 164 (2014).
7. 45 C.F.R. § 164.502 (2014); 45 C.F.R. § 164.508 (2014); 45 C.F.R. § 160.103 (2014).
8. 45 C.F.R. § 160.103.
9. American Recovery and Reinvestment Act of 2009, 41 U.S.C. § 17934 (2014).
10. *Id.* at §§ 17934, 17937.
11. 45 C.F.R. § 164.506(c) (2014); 45 C.F.R. § 164.508(a)(2) (2014).
12. 45 C.F.R. § 164.501 (2014).
13. 45 C.F.R. § 164.512(i) (2014).
14. 45 C.F.R. § 164.501(i). The preamble to the Privacy Rule explicitly included within the definition of research the development (building and maintenance) of a repository or database for future research purposes. 67 Fed Reg 53,231, (Aug. 14, 2002).
15. 45 C.F.R. § 164.514 (2013).
16. 45 C.F.R. §§ 164.512(i); 164.514(e).
17. 45 C.F.R. § 164.514.
18. 45 C.F.R. § 164.502 (e).
19. 45 C.F.R. § 164.502(b).
20. *See* 45 C.F.R § 164.502.
21. *See* 45 C.F.R. § 164.504 (2013).
22. *See* United States Dep't of Health and Human Servs., *Frequently Asked Questions: Health Information Privacy* (Dec. 15, 2008), http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/544.html. The FAQ states:

    > May a health information organization (HIO), acting as a business associate of a HIPAA covered entity, de-identify information and then use it for its own purposes?
    >
    > Answer:
    >
    > A HIO, as a business associate, may only use or disclose protected health information (PHI) as authorized by its business associate agreement with the covered entity. See 45 C.F.R. § 164.504(e). The process of de-identifying PHI constitutes a use of PHI. Thus, a HIO may only de-identify PHI it has on behalf of a covered entity to the extent that the business associate agreement authorizes the HIO to do so. However, once PHI is de -identified in accordance with the HIPAA Privacy Rule, it is no longer PHI and, thus, may be used and disclosed by the covered entity or HIO for any purpose (subject to any other applicable laws.
    >
    > The Coalition also had a meeting with OCR officials on August 7, 2013, in which the agency confirmed that patient authorization is ***not*** required if a Registry properly de-identifies PHI for research purposes as long as doing so is authorized by the Covered Entity that submitted the data. OCR re-iterated this position at a conference on registry issues sponsored by the American Medical Association's National Quality Registry Network on April 22, 2014 ("NQRN Conference").
23. 45 C.F.R. § 164.512(i).
24. *Id*.
25. United States Dep't of Health and Human Servs., *Health Services Research and the HIPAA Privacy Rule*, Nat'l Inst. of Health (May 20, 2005), http://privacyruleandresearch.nih.gov/healthservicesprivacy.asp.
26. A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. *See* 45 CFR 164.501.
27. 45 C.F.R. § 164.512(b)(i).
28. *See* United States Dep't of Health and Human Servs*., Federal Policy for the Protection of Human Subjects ('Common Rule')*, http://www.hhs.gov/ohrp/humansubjects/commonrule/index.html (last visited January 15, 2015).
29. 45 C.F.R. § 46.101(a) (2014).
30. 45 C.F.R. § 46.102(e) (2014).
31. 45 C.F.R. § 46.101(b).
32. *See* 45 C.F.R. § 46.101(a).

33. *See* United States Dep't of Health and Human Services Office for Human Research Protection, *Federalwide Assurance (FWA) for the Protection of Human Subjects*, http://www.hhs.gov/ohrp/assurances/assurances/filasurt.html (last updated June 17, 2011).
34. United States Dep't of Health and Human Services Office for Human Research Protection, *Guidance on Engagement of Institutions in Human Subjects Research*, Section III.B.6. (Oct. 16, 2008), http://www.hhs.gov/ohrp/policy/engage08.html.
35. *See* Letter from Ivor A. Pritchard, Ph.D., Senior Advisor to OHRP Director, to Anthony L. Asher, Director of National Neurosurgery Quality and Outcomes Database, (December 29, 2011), http://www.hhs.gov/ohrp/policy/Correspondence/ohrp_12/29/2014_response_.html. OHRP confirmed these statements in a meeting with PCRC on August 7, 2013 and at the April 22, 2014 NQRN conference on registry issues. *See supra*, note 22.
36. Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 44,512, 44,521 (July 26, 2011). OHRP staff reiterated this position during the August 7, 2013 meeting with PCRC and at NQRN's April 22, 2014 conference.
37. 45 C.F.R. § 160.203 (2014).
38. CAL. HEALTH AND SAFETY CODE § 1280.15 (2014).
39. 45 C.F.R. §§ 164.404(b) and 164.410 (2014).
40. VA. CODE ANN. § 32.1-127.1:03(e) (2014).
41. 45 C.F.R. § 164.524(b) (2014).
42. The National Conference of State Legislatures has a resource tracking state statutes and regulations regarding breaches of personally identifiable information. Nat'l Conference of State Legislatures*, Security Breach Notification Laws*, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Jan. 12, 2015).
43. Restatement (Second) of Torts § 652D (1977); *see e.g., Roe v. Cradduck*, 555 N.E.2d 1155, 1157 (Ill. App. 3d 1990) (noting that the Supreme Court of Illinois has acknowledged the public disclosure of private facts as a valid claim under Illinois law).
44. 17 U.S.C. § 103(b). *See also Feist Publications, Inc., v. Rural Telephone Service, Co., Inc.*, 499 U.S. 340 (1991).
45. 21 C.F.R. § 803 *et seq*.
46. 21 C.F.R. § 803.3 (2014).
47. 21 C.F.R. § 803.1(a) (2014).
48. 21 C.F.R. § 803.3.
49. 21 C.F.R. §§ 803.1; 803.10 (2014).
50. 21 C.F.R. § 803.1.
51. 21 C.F.R. § 803.3.
52. 21 C.F.R. § 803.10(c); *see also* 21 C.F.R. § 803.50 (2014).
53. 21 C.F.R. § 803.3.
54. 21 C.F.R. §§ 803.1, 803.10, 803.30 (2014).
55. 21 C.F.R. §§ 803.1, 803.10, 803.40 (2014).
56. In fact, when registries have been mentioned in products liabilities cases, it is usually to chastise a manufacturer for either not using a registry as part of post-market surveillance or for ignoring the data submitted to a registry as part of post-market surveillance. *See e.g., Fraser v. Wyeth*, 857 F. Supp. 2d 244 (D. Conn. 2012); *Barrow v. Bristol Myers Squibb,* 1998 WL 812318 (M.D. Fl. Oct. 29, 1998).
57. *See, e.g., Hempstead v. General Fire Extinguisher Corp., 269 F. Supp. 109 (D. Del. 1967) (holding that an underwriters' Laboratories could be liable for negligent approval of fire extinguisher if it's negligence was the proximate cause of an explosion that injured plaintiff); Hanberry v. Hearst Corporation*, 276 Cal. App. 2d 680 (Cal. Ct. App. 1969) (holding that a defendant-publisher may be liable for negligent misrepresentation where a plaintiff purchased shoes that contained publisher's Good Housekeeping Seal of Approval but which contained defects that caused plaintiff's injury). *See also Snyder v. American Association of Blood Banks*, 144 N.J. 269 (1996) (finding a voluntary association of blood banks liable to a patient who contracted AIDS from transfused blood for negligently failing to adopt a particular test for HIV as part of the association's recommended standards). *But see*, *NNV v. American Association of Blood Banks*, 89 Cal. Rptr. 2d 885 (Cal. Ct. App. 1999) (holding that blood banks had no liability to injured third party based on failure to recommend appropriate HIV test and disagreeing with *Snyder*).
58. *See* 15 U.S.C. § 1 (2014).
59. 15 U.S.C. § 1125 (2014).
60. *Neurotron v. Med. Serv. Ass'n. of Pennsylvania.*, 254 F.3d 444, 452 (3d Cir. 2001).
61. *Id.*
62. Note that AAEM name has since been changed to the American Association of Electrodiagnostic and Neuromuscular Medicine.
63. *Neurotron v. Am. Ass'n of Electrodiagnostic Med.*, 48 Fed. Appx. 42, 44 (4th Cir. 2002) (citing *United States v. Edge Broadcasting Co.*, 509 U.S. 418, 426 (1993)).
64. *Id.*
65. *Id.*
66. *American Society of Mechanical Engineers, Inc. v. Hydrolevel Corp.*, 456 U.S. 556 (1982) (holding that a nonprofit association violated antitrust laws when members of its standard setting council intentionally set standards to exclude certain types of manufacturers from the market for safety devices used in water boilers).

67. A third-party subpoena is one that is issued by a party in a lawsuit to a non-party that has information that the issuing party believes to be germane to the suit. *See* FED. R. CIV. P. 45.
68. *Id.*
69. *See e.g. McKinley v. Fed. Hous. Fin. Agency*, 789 F. Supp. 2d 85, 90 (D.D.C. 2011).
70. FED. R. CIV. PRO. 27–34.
71. FED. R. CIV. PRO. 26(c).
72. *See, e.g., Farnsworth v. Proctor & Gamble*, 758 F.2d 1545, 1547–48 (11th Cir. 1985) (stating that the interests against disclosing the names of patients participating in a CDC registry outweighed Proctor and Gamble's need for disclosure of the personal information of the registry participants); *Deichtman v. E.R. Squibb & Sons*, 740 F.2d 556, 564–65 (7th Cir. 1984) (finding the interests of protecting patient information in a University-sponsored registry outweighed the company's need for discovery).
73. *See Johnson v. Thompson*, 971 F.2d 1487 (10th Cir. 1992).
74. FED. R. EVID. 404.
75. 758 F.2d 1545 (11th Cir. 1985).
76. 740 F.2d 556 (7th Cir. 1984).
77. *Id.* at 566.
78. *Wolpin v. Philip Morris*, 189 F.R.D. 418 (C.D. Cal. 1999).
79. 45 C.F.R. §164.512(e).
80. 45 C.F.R. §164.502.
81. 42 U.S.C. §§ 299b-2, 299b-26. Patient safety work product means "any data, reports, records, memoranda, analyses (such as root cause analyses), or written or oral statements—
    i. Which—
        I. are assembled or developed by a provider for reporting to a patient safety organization and are reported to a patient safety organization; or
        II. are developed by a patient safety organization for the conduct of patient safety activities; and which could result in improved patient safety, health care quality, or health care outcomes; or
    ii. which identify or constitute the deliberations or analysis of, or identify the fact of reporting pursuant to, a patient safety evaluation system.

    Id. at 42 U.S.C. § 299b–21(7)(A).

    Patient safety work product does not include—
    i. Information described in subparagraph (A) does not include a patient's medical record, billing and discharge information, or any other original patient or provider record.
    ii. Information described in subparagraph (A) does not include information that is collected, maintained, or developed separately, or exists separately, from a patient safety evaluation system. Such separate information or a copy thereof reported to a patient safety organization shall not by reason of its reporting be considered patient safety work product.
    iii. Nothing in this part shall be construed to limit—
        I. the discovery of or admissibility of information described in this subparagraph in a criminal, civil, or administrative proceeding;
        II. the reporting of information described in this subparagraph to a Federal, State, or local governmental agency for public health surveillance, investigation, or other public health purposes or health oversight purposes; or
        III. a provider's recordkeeping obligation with respect to information described in this subparagraph under Federal, State, or local law.

    Id. at 42 U.S.C. § 299b–21(7)(B).
82. 42 U.S.C. § 299b-22.
83. 42 U.S.C. §§ 299b-21(2), 229b-24.
84. 42 U.S.C. § 299b-22.
85. *Id.*; 42 U.S.C. §299b-24; 42 C.F.R § 3.306 (2014); 42 C.F.R. § 3.308 (2014).
86. 42 C.F.R. §§ 3.206(a); 3.20 (2014).
87. 42 C.F.R. §§ 3.108(b)(3); (c)(2)(ii) (2014).
88. *Tibbs v. Bunnell*, No. 2012-SC-000603-MR at 13 (Ky. Aug. 21, 2014) (quoting 42 U.S.C. § 299b-21(7)(B)).
89. *Tibbs,* No. 2012-SC-000603-MR at 21–22 (citing 902 KAR 20:016 § 3).
90. *Id.*at 23. In dissent Justice Abramson disagreed, concluding that the PSO privilege "protect[s] provider safety data until it is published somehow outside the patient safety system," for example, through a hospital record or report actually submitted to the government, and precludes the "invasion of the patient safety evaluation system itself." *Id.* at 33–36.
91. *Charles v. Southern Baptist Hospital of Florida*, No. 16-2012-CA-002677 at 8 (Fla. Cir. Ct. Jul. 30, 2014)
92. *Id.* at 9. *See also* 73 Fed. Reg. 70,732, 70,742 (Nov. 21, 2008).
93. *Id.* at 8–9.
94. Susan Greene Merewitz, *Memorandum on Statutory Confidentiality Protection of Research Data*, AGENCY FOR HEALTHCARE RESEARCH AND QUALITY (Apr. 16, 2001), http://archive.ahrq.gov/fund/datamemo.htm.

95. Steven Suydam, et al., *Patient Safety Data Sharing and Protection from Legal Discovery*, 3 ADVANCES IN PATIENT SAFETY 361, 363 (2005), *available at* http://www.ahrq.gov/professionals/quality-patient-safety/patient-safety-resources/resources/advances-in-patient-safety/vol3/Suydam.pdf .
96. *Contra* 42 U.S.C. § 241(d) (2013) (stating that the Secretary of HHS may authorize individuals involved in HHS-sponsored research to protect the identity of their subjects and stating that such information is not discoverable). For more information on the Certificates of Confidentiality discussed in 42 U.S.C. § 241(d), see § II(e), *infra*.
97. United States Dep't of Health and Human Servs., *Certificates of Confidentiality: Background Information*, NAT'L INST. OF HEALTH, http://grants2.nih.gov/grants/policy/coc/background.htm (last updated Jan. 20, 2011). *See also* United States Dep't of Health and Human Servs., *Certificates of Confidentiality: Frequently Asked Questions*, HEALTH RES. AND SERV. ADMIN., http://www.hrsa.gov/publichealth/clinical/HumanSubjects/faqs.html (last visited Sept. 1, 2014).
98. 42 U.S.C. § 241(d) (2014).
99. United States Dep't of Health and Human Servs., *Certificates of Confidentiality: Background Information*, NAT'L INST. OF HEALTH, http://grants2.nih.gov/grants/policy/coc/background.htm (last updated Jan. 20, 2011).
100. United States Dep't of Health and Human Servs., *Frequently Asked Questions: Certificates of Confidentiality*, NAT'L INST. OF HEALTH, http://grants.nih.gov/grants/policy/coc/faqs.htm (last revised June 20, 2011).
101. *Id.*
102. *Id.*
103. *See, e.g.*, Illinois Medical Studies Act, 735 ILL COMP. STAT. 5/8-2101 (2014).
104. *Application of American Tobacco Co.*, 880 F.2d 1520, 1528 (2d Cir. 1989) (citing *Deitchman*, 740 F.2d at 560–61) (holding that in New York there was no such "scholar's privilege").
105. 672 F.2d 1262 (7th Cir. 1982).
106. 162 F.3d 708 (1st Cir. 1998).
107. *Id.* (citing *In re Madden*, 151 F.3d 125, 12–31 (3d Cir. 1998)); *Shoen v. Shoen*, 5 F.3d 1289, 1293–94 (9th Cir. 1993); *von Bulow v. von Bulow*, 811 F.2d 136, 142–44 (2d Cir. 1987).
108. *See e.g.*, *Humane Society of the United States v. Superior Court of Yolo County*, 214 Cal. App. 4th 1233 (Cal. App. 2013).

