The Application of HIPAA and the Common Rule to Clinical Registries

Completed by the NQRN®, a program of the PCPI®

This document is only intended to be a summary of the uses of information from clinical registries for quality improvement and research purposes, as they relate to the “Health Insurance Portability and Accountability Act of 1996” (HIPAA) and the “Federal Policy for the Protection of Human Subjects” (Common Rule). All users of this document should refer to the U.S. Department of Health and Human Services (HHS) websites for complete requirements:

http://www.hhs.gov/ocr/privacy/
http://www.hhs.gov/ohrp/humansubjects/commonrule/

The PCPI Foundation, including the NQRN, disclaims any liability for use or non-use of this document. The PCPI does not provide medical, legal, financial, or other professional advice and users are encouraged to consult a professional for such advice.

©2015 The PCPI Foundation. All rights reserved.
Credits and Acknowledgements

The NQRN gratefully acknowledges its Research and Privacy Task Force which provided content, input and guidance to the development of this document.

Anthony Asher, MD (chair)  Kavitha Neerukonda, JD
American Board of Neurological Surgery  American Academy of Physical Medicine and Rehabilitation

Mark Barnes, JD, LLM  Sally Okun
Ropes & Gray LLP  PatientsLikeMe

Mark Fox  Rob Portman, JD
American College of Cardiology  Powers Pyles Sutter & Verville PC

Tom Granatir  Josh Rising, MD
American Board of Medical Specialties  The Pew Charitable Trusts

Norman Kahn, MD  Jill Sage, MPH
Council of Medical Specialty Societies  American College of Surgeons

Audiey Kao, MD, PhD  Jessica Sutin, JD
American Medical Association  UnitedHealthcare

Art Levin, MPH
Center for Medical Consumers

The Task Force acknowledges the valuable contributions of:

Sarah Imhoff, JD, MHSA  Amita Sanghvi, JD, MHA
Powers Pyles Sutter & Verville PC  Powers Pyles Sutter & Verville PC

PCPI Staff:

Seth Blumenthal, MBA
NQRN Program Manager
Table of Contents

Credits and Acknowledgements................................................................................................................................................... 2
Introduction.................................................................................................................................................................................... 4
Background on the application of HIPAA and the Common Rule to registries ................................................................. 6
    HIPAA ................................................................................................................................................................................... 6
    Common Rule ................................................................................................................................................................. 7
Application of HIPAA and the Common Rule to registry activities......................................................................................... 9
    HIPAA ................................................................................................................................................................................... 9
    Common Rule ................................................................................................................................................................. 10
        Common Rule aspects for providers submitting data to registries for research.................................................. 10
        Common Rule aspects for registries receiving data from providers for research ........................................ 10
Quality Improvement ............................................................................................................................................................. 12
Appendix A: Recommended expertise .................................................................................................................................. 14
Appendix B: Decision trees .................................................................................................................................................. 15
Bibliography ........................................................................................................................................................................... 18
Introduction

A broad interest in understanding health care value, combined with the rapidly increasing availability of electronic health data, have increased the demand for specific, timely information on quality and performance. Clinical data registries are responding to this need by providing rich, trustworthy data that are useful for physicians, health care professionals and others to make decisions that improve health and health care.

Clinical data registries record information about the health status of patients and the health care they receive over varying periods of time. Clinical registries typically focus on patients who share a reason for needing health care. They allow health care providers and others to see what treatments are available, and how patients with different characteristics respond to various treatments. This information can be used to inform patients and their health care professionals as they decide the best course of treatment and to improve care for patients in the future. Information from registries may also be used to compare the performance of health care providers with regard to the outcomes of and resource use associated with the care they deliver. (1)

As registries collect detailed information about a patient’s health care treatment and outcomes, various federal and state health privacy and security laws apply to the use and disclosure of a patient’s identifiable health information. For instance, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH”), and the regulations implemented thereunder (collectively, the “HIPAA Regulations”), protect the privacy and security of a patient’s protected health information (“PHI”). (2)

When a registry conducts federally-funded or federally-regulated research involving human subjects (“human subjects research”), informed consent, assurances of compliance and Institutional Review Board (“IRB”) review and approval may be required in order to ensure that the human subjects understand the risks of the research and the research processes, and that procedures meet ethical and legal standards. The Federal Policy for the Protection of Human Subjects, popularly known as the “Common Rule,” which has been promulgated in separate regulations by fifteen federal departments and agencies and is followed by three others, outlines the ethical standards for human subjects research and protects the privacy, including identifiable private information, of human subjects. In proposed rulemaking published in the Federal Register on September 8, 2015, multiple federal agencies proposed expansive changes to the Common Rule and its implementing regulations. Some of the proposed changes, if finalized in their current form, will affect registries including, but not limited to, research conducted by registries. (3) (4) (5) (6)

Because it is often difficult to make the distinction between research and quality improvement, the latter efforts may sometimes be subjected to research standards applicable only to the former. Present standards surrounding human subjects research and patient privacy (governed by the Common Rule and HIPAA Regulations, respectively) are more developed and specific than those for quality improvement. This is particularly the case when aspects of quality improvement activity using registry data overlap with elements typically found in traditional clinical research. For example, it is increasingly recognized that both longitudinal data and patient-reported outcomes are fundamental to the comprehensive assessment of the quality and appropriateness of specific clinical interventions. Longitudinal data make it possible to determine the durability of treatment effects, while patient-reported outcomes create a more
comprehensive picture of the quality of care received. The need for data collection extending beyond acute care settings, and interactions with patients to obtain prospective outcomes data, have raised questions about the applicability of research regulations to these activities.

The NQRN is committed to advancing a shared understanding of how to fully leverage the value contained within registry data for improving patient health outcomes. It seeks to eliminate hurdles for quality improvement, patient safety initiatives and clinical research programs, while at all times protecting the privacy and security of PHI. The NQRN, through its Research and Privacy Task Force (“Task Force”) wishes to provide clarity by highlighting existing guidance that applies to uses of information from registries. Where current guidance is not clear, the Task Force has attempted to provide additional insight to allow registry stewards and users of information from registries to extract full value from these data systems while protecting privacy and security. Although we attempt here to provide a detailed summary of registry uses and the implications of HIPAA and the Common Rule, certain areas of expertise are necessary to successfully navigate the registry privacy and security landscape. This expertise may be brought in-house or outsourced as needed. Consultation with a qualified attorney is recommended. (Appendix A – Recommended Expertise)

The Task Force has also developed decision trees to assist registry operators and users in determining what, if any, aspects of HIPAA and the Common Rule apply. (Appendix B – Decision Trees)
Background on the application of HIPAA and the Common Rule to registries

HIPAA

The HIPAA Regulations protect the privacy of a patient’s PHI. The HIPAA Regulations consist of, among other things, a Privacy Rule, which sets the standards for the use and disclosure of PHI, and a Security Rule, which specifies the administrative, physical, and technical safeguards and documentation requirements to ensure the protection of PHI. (2) (7)

PHI is information that is a subset of health information, including demographic information collected from an individual, that:

1. Is created, received, maintained, or transmitted by a health care provider, health plan, employer, or health care clearinghouse (collectively, “covered entities”);
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
3. Identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual that is:
   a. transmitted by electronic media;
   b. maintained in electronic media; or
   c. transmitted or maintained in any other form or medium. (8)

The HIPAA Regulations apply to “covered entities” and their “business associates,” which include subcontractors with access to PHI that are working on behalf of a business associate. Organizations that participate in registries are typically hospitals, group practices and other health care facilities, and are covered entities under the HIPAA Regulations. We refer to such organizations throughout this document as registry “participants.” Business associates are persons or entities that provide services for or perform functions on behalf of a covered entity (or a covered entity’s business associate), where the person or entity has access to the covered entity’s (or its business associate’s) PHI. Registries typically function as business associates of a physician, hospital or other provider when they support quality improvement efforts and the health care operations of such providers through data collection, data aggregation, and data analysis, including benchmarking.

The use or disclosure of PHI by a covered entity or business associate requires patient authorization unless disclosure falls within one of several exceptions. The Privacy Rule allows for the disclosure of PHI by a covered entity without patient authorization for the purpose of “health care operations.” Health care operations include quality assessment and improvement activities, which can involve data aggregation and outcomes evaluation, as long as the development of generalizable knowledge is not the primary purpose of such activities. Covered entities may also disclose PHI to their business associates for the purpose of permitting the business associate to use the PHI to perform a payment or health care operations function on behalf of the covered entity, provided that the parties have first entered into a HIPAA-compliant Business Associate Agreement (“BAA”). Additional permitted exceptions may apply. (2)

Research is not considered “health care operations” under HIPAA. Accordingly, when PHI is disclosed for research purposes, the Privacy Rule requires a legal basis for the disclosure, such as a patient’s
In order to obtain an IRB or privacy board alteration or waiver of HIPAA authorization, the following conditions must be met:

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. (10)

When evaluating if HIPAA patient authorization will be required, the level of data that will be captured must be evaluated. A Limited Data Set (“LDS”) is information that is partially de-identified by removing all direct identifiers, but retains only certain indirect PHI, such as an individual’s age, or city, state, or zip code, and all elements of dates. If the research is conducted using a LDS, patient authorization is not necessary. However, if the research requires more than a LDS it will need to be determined if the research qualifies for a waiver of HIPAA authorization. It should also be noted that no authorization is required for the use or disclosure of PHI of decedents for research purposes. Thus if a registry conducts research solely on information of decedents, it could use and disclose PHI of such decedents without HIPAA authorization or waiver of authorization. (2)

In most instances retrospective research will meet all the requirements for a waiver of HIPAA authorization. However in the instance of prospective research, most studies will not meet the requirements for a waiver of HIPAA authorization because, due to the nature of the research design, the investigators have an opportunity to obtain authorization from the subjects.

It is also important to note that many IRBs are unfamiliar with registries, and it is therefore often necessary to provide an IRB with detailed information pertaining to registry operations to facilitate accurate determinations in response to requests for waivers of HIPAA authorization.

**Common Rule**

When a registry or one of its participants conducts human subjects research, informed consent, assurances of compliance, and IRB review may be required in order to ensure that the human subjects understand the
risks of the research, and that the research processes and procedures meet ethical standards. The Common Rule outlines the ethical standards for human subjects research. Under the Common Rule, a “human subject” is defined as “a living individual about whom an investigator conducting research obtains:

1. Data through intervention or interaction with the individual, or
2. Identifiable private information.”

Human subjects may also include vulnerable populations, such as children, prisoners, pregnant women, mentally disabled persons, or economically or educationally disadvantaged persons. (11) (12)

The Common Rule applies to human subjects research that is federally-funded or conducted subject to federal regulations. “Research subject to regulation” is defined as “research activities for which a federal department or agency has specific responsibility for regulating as a research activity.” For example the National Institutes of Health (“NIH”) is responsible for regulating any research activity carried out under a NIH-issued federal award. The Common Rule generally does not apply to privately-funded research activities not otherwise subject to federal regulation unless an institution has elected in its federalwide assurance to apply the Common Rule to all of its human subjects research, regardless of funding source. This election is sometimes known as “checking the box.” (11) (13)
Application of HIPAA and the Common Rule to registry activities

HIPAA

The extent to which the HIPAA Regulations apply to registry activities will depend on the purpose of the collection and the type of data collected.

The purpose for which the data are collected is the first consideration. If a registry is collecting PHI primarily for health care operations purposes, the entity controlling the registry and each of the registry’s other participant entities need to enter into a BAA. For example, if the registry will be performing analyses with the PHI that support the participant entities’ health care operations, such as providing the participant entities with benchmarks and specific information about their quality outcomes, and if such function requires the disclosure of full PHI, then a BAA is required. If the registry will be combining PHI from multiple participant entities in order to provide such services, the BAA must authorize explicitly the registry to engage in “data aggregation” functions. The type of data collected by a registry is another relevant factor when evaluating the application of HIPAA to the registry. A registry’s use or disclosure of de-identified information is not governed by HIPAA. De-identified health care information is that from which either (a) 18 identifiers listed in the Privacy Rule have been removed, or (b) information that has undergone a process of statistical de-identification in accordance with regulations. If a registry obtains only de-identified information to perform health care operations activities for its participants, then no BAA is required. If the registry obtains an LDS in order to perform health care operations activities for its participants, then a Data Use Agreement (“DUA”) should be executed by the entity controlling the registry and by the covered entity providing the LDS. When the only PHI that the participant covered entity discloses to the registry is in the form of an LDS, the DUA may be used in place of the BAA. If the registry will receive and use both limited data sets and fully-identified PHI, a combined BAA/DUA may be required.

If the registry wishes to use PHI for research purposes, HIPAA’s research rules become relevant. If the registry obtains fully-identified PHI solely for research purposes, or obtains PHI for health care operations purposes but also wishes to use such fully-identified PHI for research purposes, the authorization of the patient or a waiver of authorization from an IRB or privacy board will generally be required. If the registry will collect data prospectively, the covered entity contributing PHI to the registry could obtain the patient’s authorization for the disclosure and use of the PHI. Alternatively, if the criteria discussed above for a waiver of authorization are met, the registry could obtain IRB/privacy board waiver of HIPAA authorization. If granted by the registry’s IRB/privacy board, such waiver could be relied on as a basis for disclosure of PHI by all participant covered entities providing data to the registry. That is, the law does not require that the participant entities obtain separate waivers from their local IRBs. Of course, registry participant entities may still insist on obtaining local IRB approval or waivers to comply with their institutional policies. Registries collecting retrospective data can usually provide evidence to support an IRB or privacy board granting a waiver of authorization. (14)

Alternatively, if the registry has obtained PHI for health care operations purposes but wishes to create de-identified data or limited data sets from such PHI for research purposes, the registry may be able to do so without obtaining patient authorization or waiver of authorization. In order for such activity to be permissible, the registry’s BAA with the covered entities contributing data to the registry must explicitly
permit the registry to de-identify data for research purposes and/or create limited data sets. In the case in which limited data sets are created, a DUA between the entity controlling the registry and the covered entity providing the LDS would also be required.

**Common Rule**

**Common Rule aspects for providers submitting data to registries for research**

Of particular interest to clinical data registries, the Office for Human Research Protections (“OHRP”), the office within HHS that administers the Common Rule, has clearly stated that entities that collect data in the course of clinical care and submit that data to external researchers are not themselves 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, “institutions 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 themselves engaged in human subjects research, but institutional requirements or other regulations may still apply. OHRP has further indicated that this guidance applies to hospitals, physician groups, and other entities otherwise covered by the Common Rule that are only submitting data to registries in the normal course of treating patients and are not themselves performing research on the data. 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. (14) (15)

OHRP has stated, however, that an entity is engaged in human subjects research when its staff collects informed consent from research participants. Accordingly, if a registry conducts research that is subject to the Common Rule and the informed consent for participation in the registry is collected by a staff member of a hospital or physician office, the research will need to be approved by the cognizant IRB for that hospital or physician office, or by an IRB with which the institution has entered into an authorization agreement, such as a central IRB.

**Common Rule aspects for registries receiving data from providers for research**

Federally funded human subjects research is subject to the jurisdiction of the Common Rule, requiring IRB review and informed consent or waiver of consent. When registries conduct human subjects research that is federally funded or conducted at an institution that has elected in its Federalwide Assurance to apply the protections of the Common Rule to all of its research, the Common Rule may apply to such research. In determining how the Common Rule applies to the registry, one of the first aspects to consider is if the research is conducted retrospectively or prospectively.

The Common Rule makes no distinction between the primary and secondary intents of data collection. In retrospective research, the investigator looks backward at already collected data. For a registry conducting research, retrospective research is almost always conducted as a secondary purpose. This means that the data being used for a research purpose were originally collected for another purpose, such as quality improvement. In contrast, prospective research involves the collection of data in a real-time fashion. In this instance the data collection usually occurs for the primary purpose of research, or in an instance
where the registry operator is using baseline data from a registry to supplement data collected for a research study.

Provided that the Common Rule applies, either because the registry receives federal funding or the registry operator has signed a federalwide assurance agreement in which it has elected to apply the Common Rule to all of its human subjects research, research protocols will need to be developed. A Principal Investigator (“PI”) will need to be assigned to oversee these protocols. Once the protocols that outline research plans have been written and assigned a PI, they are submitted to an IRB for review.

Registries conducting research should consider two factors when submitting an IRB protocol: does the research qualify for an exemption under the Common Rule, and is the registry participant engaged in research.

The following is a list of exemption categories:

1. Research conducted in established or commonly accepted educational settings, involving normal educational practices
2. Research involving the use of educational tests, survey procedures, interview procedures, or observation of public behavior
3. Research involving collection or study of existing data, documents, records, or pathological or diagnostic specimens
4. Research studying, evaluating, or examining public benefit or service programs
5. Research involving taste and food quality evaluation or consumer acceptance studies

The exemption that typically applies to research conducted on registry data involves the collection or study of existing data, documents, records, or pathological or diagnostic specimens. In order to meet this exemption, the research must involve only the collection or study of data, documents, records, pathological specimens, or diagnostic specimens in existence before the research is proposed to an institutional official or the IRB. Additionally, the data must be either publicly available or recorded in a way that the subjects cannot be identified, directly or through identifiers linked to the subjects. Individual institutional policies vary on how to determine if research is exempt. Some institutions require that an IRB make this determination through submission of a request for exemption determination.

Once the research protocol is approved and the consent or authorization forms are approved, if the research is non-exempt human subject research, the IRB will set the parameters for continuing review. Generally, continuing review for registry based research studies occurs annually.

The Task Force recommends that investigators keep the IRB informed of any changes or problems pertaining to a research study. Reportable aspects prior to the continuing review include but are not limited to material changes to the protocol, a change of the PI, any newly identified conflicts of interest of the research team, disciplinary action taken against the institution, PI or research team, protocol deviations, breaches of confidentiality and severe adverse events. Consulting with institutional policy and investigator handbooks for additional information can be helpful in keeping the IRB appropriately informed.

A second factor to consider is whether registry participants are “engaged” in research. OHRP released guidance which assists institutions in determining if they are engaged in research. This is important in
determining if the protocol filed with the IRB will need to be single site protocol, for only the research conducted by one registry, or a multi-site protocol where each registry participant is engaged in research.

In instances where registry participants are engaged in the research it is important to advocate for the use of a single IRB for oversight. Again, in most instances of retrospective research registry participants may not be engaged because they are simply releasing the data to an investigator for research. An IRB consultation can help in navigating the guidance. (15)

**Quality Improvement**

The HIPAA Privacy Rule states that PHI can be used to evaluate health care provider performance, or for any other purpose that meets the definition of health care operations under the Privacy Rule. Health care operations include conducting “quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that obtaining generalizable knowledge [research] is not the primary purpose of any studies resulting from such activities.” (9)

Assuming that the primary purpose of clinical registries is to advance quality assessment and improvement activities, including outcomes evaluation, the following is relevant to registries:

First, a registry that is not supported by or regulated by HHS or any other federal agency, and that has not elected to extend the application of the regulations to non-federally funded research activities via the HHS federalwide assurance, does not have to meet any of the requirements of the Common Rule, including review by an IRB, for this non-HHS funded activity. Note however, this “technical exemption” is not likely relevant due to the broad application of the Common Rule by most institutions to any activity thought to be clinical research, meaning that the proper inquiry becomes whether the registry’s activities constitute “research” within the meaning of the Common Rule. (17)

Second, practice groups collecting clinical data for the purposes of quality improvement that are disclosing private identifiable information obtained through the administration of standard clinical care to patients to a registry, are not themselves engaged in human subjects research. Importantly, OHRP has noted that provider outreach to patients in the context of therapeutic interventions, with the primary intent of quality improvement, including patient follow-up questions, would not fall within OHRP’s regulations, if the change in care would have taken place regardless of any secondary purpose (i.e., prospective research) relating to the collection of information about that change.

Third, OHRP does regard the development of national practice benchmarks (which are essential for allowing accurate comparisons of physician performance) by registries as “human subjects research” as defined by the regulations since these benchmarks are considered to be “generalizable knowledge.” If a registry operator chooses to extend Common Rule standards to non-federally funded projects, or an institution is engaged in a federalwide assurance agreement with the federal government, or if the registry is supported by federal funds, IRB review would be required, but the review could be obtained from a single IRB. Under these circumstances, it is highly likely that the registry institution would apply for an IRB waiver of informed consent. (18)

The Privacy Rule distinguishes between research, quality assessment and improvement activities based on whether the primary purpose of the study in question is to obtain generalizable knowledge. Although generalizable knowledge in the form of national benchmarks of performance will be generated by most
quality improvement registries, the primary purpose of such registries is likely to promote health care quality improvement. According to HIPAA, if the primary purpose of the studies resulting from quality assessment and improvement activities is not to produce generalizable knowledge, the covered entity may use or disclose PHI for the study without patient authorization. (19)

Finally, both OCR and OHRP have issued opinions with respect to retrospective use of de-identified data for research, a process which may advance the objectives of registries used for quality improvement purposes. OHRP does not consider the activity of using de-identified data for later research as being human subjects research as long as in the analysis researchers are obtaining de-identified data and are not intervening or interacting with the subjects in any way outside the normal course of care.

In the rare circumstance that a local IRB determines that an institution is engaged in research through participation in a registry despite the OHRP opinion that the participation of sites in these types of projects does not constitute human subjects research, it is recommended that registries modify the project description into a clinical protocol submission based on their individual IRB’s document templates. Furthermore, in these instances it is suggested that a waiver of consent be requested.

The Privacy Rule permits covered entities to use and disclose data that have been de-identified without obtaining an authorization and without further restrictions on use or disclosure because de-identified data are not PHI, and therefore are not subject to the Privacy Rule. A covered entity may de-identify data itself as part of its “health care operations,” or it may contract with a business associate to perform this function on its behalf. Importantly, it is generally permissible for a covered entity to engage a business associate to de-identify data even if the business associate is the intended recipient of the de-identified data, so long as the business associate destroys all of the identifiers and any linking codes after creating the de-identified data set.

The use of registries for the assessment of clinical and economic effectiveness of care deserves special mention. From a public policy perspective, it is important to know how one therapy prescribed for a given condition compares with another. This type of analysis, usually known as comparative effectiveness research (“CER”), is normally hypothesis-driven and is primarily intended to advance our general knowledge regarding healthcare value. As such, CER, whether conducted with traditional methods such as randomized controlled trials (“RCTs”) or as prospective registry studies, would likely fall under the jurisdiction of current research regulations (particularly the Common Rule). However, most clinical registries are not being used for that purpose (i.e., replacing RCTs for CER) and are rather directed to evaluations of individual practitioner/group and hospital performance, along with evaluations of individual patient experience. In that regard, asking questions about the effectiveness of a procedure from a patient’s perspective in the absence of a direct prospective comparison with similar patients undergoing different procedures is consistent with current definitions of “healthcare operations” as defined by HIPAA, and is critically important when evaluating care quality and individual opportunities for improvement.
Appendix A: Recommended expertise

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal</td>
<td>It is recommended that registry operators engage legal counsel to navigate privacy and human subject research laws and regulations, specifically HIPAA and the Common Rule and their application to registry data. Registry operators also need to evaluate applicable state privacy or consumer protection laws and matters concerning data ownership. The PCPI Foundation including the NQRN disclaims any liability for use or non-use of this document. The PCPI does not provide medical, legal, financial, or other professional advice and users are encouraged to consult a professional for such advice.</td>
</tr>
<tr>
<td>Health IT</td>
<td>Registry operators that are covered entities or business associate of covered entities and choose to collect PHI will need to comply with the HIPAA Security Rule with respect to such PHI. The rule requires the implementation of physical, technical, and administrative safeguards and has significant documentation requirements. It is important to engage organizational leadership including the Chief Information Officer (“CIO”) in developing data security infrastructure. If data warehousing is outsourced to a vendor, legal counsel and the CIO should still be consulted to ensure that the vendor complies with the Security Rule. It is important to remember that the Security Rule applies to all sub-contractors of a business associate who will access PHI. It is recommended that the CIO have a mechanism for ensuring that all sub-contractors comply with the HIPAA security rule. It is also recommended that registry operators engage legal counsel to navigate security laws and regulations, specifically HIPAA and its application to registry data.</td>
</tr>
<tr>
<td>Research</td>
<td>General familiarity with clinical research protocols as well as an understanding of their contribution, if any, to patient risk, is recommended.</td>
</tr>
<tr>
<td>Quality improvement</td>
<td>General familiarity with clinical quality improvement models, especially at the intersection between QI and research, is recommended</td>
</tr>
</tbody>
</table>
Appendix B: Decision trees

Instructions for use:

Registries: Use the decision trees together as a set, beginning with the HIPAA tree:

- Begin by making a list of all organizations involved in operating or participating in the registry that use or disclose PHI.
- Understand the type of data used, transferred to/from each organization, and the specific activities each entity carries out on the data (e.g., de-identification).
- Traverse the HIPAA decision tree and learn which business associate agreements are required and if patient authorization is needed to use PHI.
- Next, determine primary and expected secondary uses of registry data (e.g., quality improvement).
- Traverse the Common Rule decision tree to understand if the Common Rule applies, if IRB review is needed, and if patient consent exceptions may apply to expected primary and secondary uses. When crafting the necessary agreements, it is important to anticipate to the degree possible the registry data uses now and in the future, so that the need to obtain patient authorization or consent in the future, which may be difficult, is minimized.
Does HIPAA apply?

Start here

Does the activity use only de-identified data?

Yes

No

Does the registry use or disclose only a limited data set (LDS) for research, public health or health care operations purposes?

Yes

No; LDS for Other purposes

Does the registry use or disclose full protected health information (PHI) on behalf of a covered entity (CE)?

Yes

Is the activity for treatment, payment or health care operations or one of the business associate functions listed in the HIPAA Privacy Rule (e.g., legal, accounting, consulting)?

No

Yes

A data use agreement (DUA) is required between the registry and the CE. No patient authorization needed.

Patient authorization is generally required.

Business associate agreement (BAA) is required between the registry and the CE. No patient authorization needed.

Patient authorization or IRB waiver or alteration of authorization is required

HIPAA does not apply

Sources: (2) (20) (21)

Other federal, state, local laws and/or regulations may also apply.
Does the Common Rule apply?

Start here

Is the activity a systematic investigation designed to develop or contribute to generalizable knowledge?

Yes; the activity is research

Is the research obtaining information about living individuals?

Yes

Does the research involve intervention or interaction with the individuals?

Yes

Is the research conducted or supported by the U.S. Department of Health & Human Services?

Yes

Is the research covered by a federalwide assurance agreement?

Yes

The Common Rule applies and IRB oversight is required unless the research is exempt under 45 CFR 46.101 (b)

No

The Common Rule does not apply, but other federal, state, local laws and/or regulations may apply

No

Is the information individually identifiable?

No

Is the information private?

Yes

The Common Rule applies and IRB oversight is required unless the research is exempt under 45 CFR 46.101 (b)

No

Sources: (22) (16) (11) (23). Other federal, state, local laws and/or regulations may also apply.
Bibliography


10. —. Privacy of Individually Identifiable Health Information, Uses and disclosures for which an authorization or opportunity to agree or object is not required, 45 C.F.R. § 164.512. Code of Federal Regulations. 2013.


