



Legal and Ethical Architecture for PCOR Data

CHAPTER 4:

FRAMEWORK FOR NAVIGATING LEGAL AND ETHICAL REQUIREMENTS FOR PCOR

Submitted by:

The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

11	NTRODUCTION	1
PCOR FRAMEWORK1		
	Data Characteristic 1: Identifiability	4
	Data Characteristic 2: Content	6
	Data Characteristic 3: Subject	8
	Data Characteristic 4: Source	11
	Data Characteristic 5: Access	13
	Data Characteristic 6: Use/Purpose	16
	Data Characteristic 7: Consent/Authorization	19
	Data Characteristic 8: Security	23
	Data Characteristic 9: Legal Status	



Chapter 4

Framework for Navigating Legal and Ethical Requirements for PCOR

INTRODUCTION

Building on Chapters 2 and 3, this chapter presents a visual decision tool that highlights the key considerations associated with the spectrum of data used for PCOR and the nature of the relationships between researchers and other stakeholders. This Framework is built on the data characteristics and types (discussed in the previous chapters) that are critical to navigating legal and ethical requirements that govern use and exchange of data for PCOR.

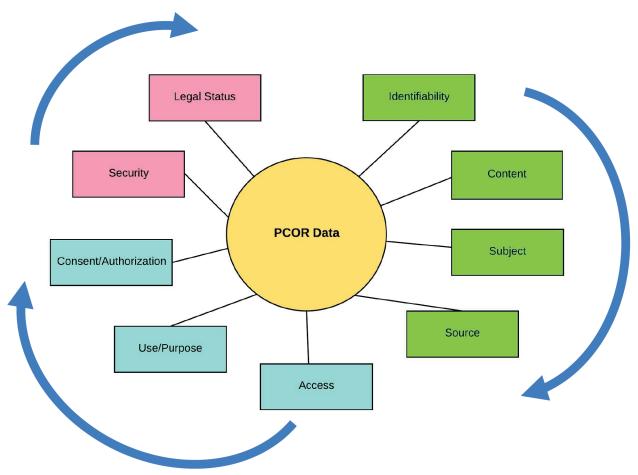
PCOR FRAMEWORK

This Framework is designed to serve as a decision tool for PCOR researchers that addresses the key data characteristics and considerations (previously discussed in Chapter 2) both individually and collectively. While the characteristics presented here are by no means exclusive, they represent the key characteristics of data that determine what legal requirements and ethical principles apply for research use of that data.

- Identifiability: Refers to the ability to link information to particular individuals.
- Content: Refers to the subject matter or substance of the data.
- Subject: Refers to the person or thing that is the focus of the data.
- Source: Refers to the person, entity, and/or setting in which the data originated or was collected.
- Access: Refers to the ability of a person or entity other than the individual subject(s) of the information to view, create, edit, or share data.
- Use/Purpose: The intended use or purpose of the data collection will affect whether and how the data may be collected and used.
- Consent/Authorization: Refers to the activities and documentation potentially required of researchers seeking permission to collect, use, or share data about an individual.
- Security: Refers to the means by which data is protected from unauthorized use or access.
- Legal Status: Refers to rights and responsibilities related to data that may be triggered by ownership rights, agency principles, and/or contractual obligations.

These characteristics are not mutually exclusive, and the considerations that surround them are interconnected and frequently overlapping. For example, ownership of a certain data set under the terms of a contract (which is an aspect of "legal status") also determines who may access the data; the content and subject characteristics of data affect how it may be used; and identifiability may determine what consent or authorization must be obtained in order to use the data for research. Users are encouraged to review all of the characteristics thoroughly to determine if/how they apply to their research.

As discussed in Chapter 2, answers to key questions related to these characteristics can help researchers understand the legal and ethical significance of different aspects of data used for PCOR. These data characteristics are displayed as the spokes around a wheel, with the center of the wheel representing PCOR data.



For this chapter, the key characteristics are organized into three color-coded groups according to their priority for decision-making by researchers and are organized around the wheel in the order in which a researcher should consider them, starting with "Identifiability" in the top right position and moving clockwise around to "Legal Status."

Step One: The lime-colored characteristics (Identifiability, Content, Subject, and Source) are the factors that determine whether a statute or regulation applies to the data. A researcher should consider these characteristics first because determinations associated with these characteristics will inform a researcher whether and what statutes and regulations potentially apply and also inform the researcher of the need to move on to the second step for consideration. For example, if a researcher determines that the data in question is identifiable, several statutes and regulations potentially apply, and their requirements will depend on secondary considerations such as Access and Use/Purpose. If a researcher determines that the data is de-identified, then no statute or regulation applies to the data, and the researcher will not need to consider the secondary considerations.

Step Two: The aqua-colored characteristics (Access, Use/Purpose, and Consent/Authorization) are issues that address how a researcher should navigate statutes and/or regulations that apply to the data in question. If a statute and/or regulation applies, the collection or use of the data may be limited or restricted by requirements related to these characteristics.

Step Three: The pink-colored characteristics (Security and Legal Status) involve case-specific determinations relating to data collection and use by a PCOR researcher. For each research protocol, a researcher should consider these characteristics separate and apart from the considerations discussed in steps one and two to the extent they apply. In all cases (as noted at the bottom of each diagram), a researcher should consult with legal counsel (in-house or external), IRB policies and practices, and organizational policies and procedures.

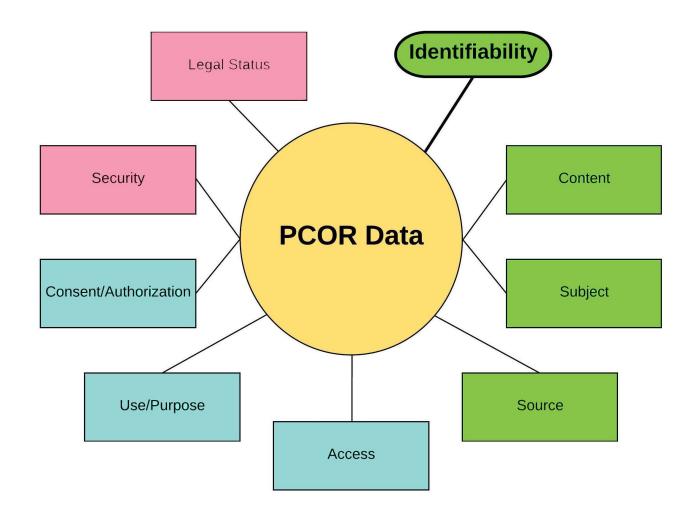
Each characteristic is further explored individually in a decision-oriented structure that illustrates key questions and considerations related to each data characteristic:

- *Key Question:* The content in this column identifies the key questions related to a data characteristic that a researcher must address.
- What It Means: The content in this column identifies the meaning and/or interpretation of the key questions related to PCOR.
- Why It Matters: The content in this column identifies the legally significant aspects of the issue raised by the question, including identification of any relevant statutes and regulations that are potentially implicated by the issue.
- Considerations for Next Steps: The content in this column identifies legal and ethical considerations
 and activities for PCOR researchers related to each question, including implications for structuring
 research.
- General Note: At the end of each data characteristic's structure are reminders to ensure that
 research complies with relevant legal and ethical requirements and to identify the parties to consult
 for further guidance.

This chapter is designed to be a decision tool for PCOR researchers guiding them through a series of considerations specific to the key characteristics that determine whether laws apply to particular data and if so, what requirements attach to collection and use of the data. Potentially applicable laws are referenced throughout the Framework, and complete summaries of key laws are included in Appendix A.

It is important to note that, by design, this chapter does not delve into the complex legal requirements as do Chapters 1, 2, and 3. Rather, as noted above, this chapter provides a decision guide for PCOR researchers to help them understand both the independence and interconnectedness of the characteristics associated with relevant data and a suggested model for assessing and understanding those issues, their relationship to relevant statutes and regulations, and next steps.

Data Characteristic 1: Identifiability



<u>Identifiability</u>

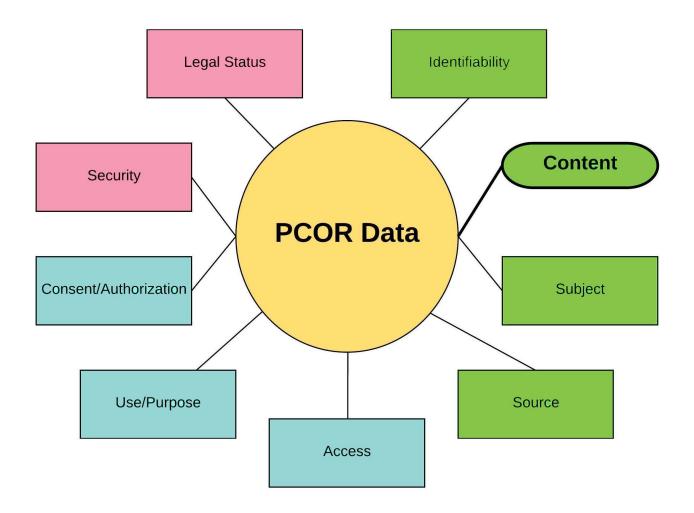
Identifiability refers to the ability to link information to particular individuals.

Identifiability pg. 2 Considerations **Key Question** What It Means **Why It Matters** for Next Steps* What information Identifying data elements are those Health-related data that contains any Consider whether does the data that allow the user to link the identifying information may be subject the data you wish to contain? Does this information to the individual subject to the health information privacy use for your information directly of the information. These elements framework. Even a data set stripped of research must be in identify individuals? can be direct identifiers (e.g., an most direct identifiers such as a limited identifiable form and data set, is considered identifiable individual's name, social security what requirements number) or can be indirect identifiers because one or more direct identifiers apply to your use of (e.g., information that, when taken are present. Laws and regulations that that data. as a whole or when combined with define identifiability and protect certain types of identifiable information other available information, can be used to identify an individual). include: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA state law. Consider whether Has the data been Information that was once De-identified data is generally not de-identified? If so. identifiable but has been stripped of subject to the health information the data you wish to how? any elements that directly identify privacy framework. In general, deuse for your the individual or could be used to identified data has either been stripped research has been identify the individual s considered of specific identifying elements or has de-identified and "de-identified.' The process by which been deemed "de-identified" by an whether this process de-identification occurs is relevant to expert. Laws and regulations that meets applicable determining whether or not define de-identified data and set forth legal standards. information meets applicable requirements for it include: HIPAA, definitions of "de-identified." Common Rule. Part 2. state law. Can the data be re-Data that has been stripped of all If a user knows that de-identified data Consider whether identifying information may include a identified when could still be used to identify the there is other combined with data key or code that allows certain users individual in some way, there may be available information from another to link the de-identified information limitations on how and to whom the or a key that would source? back to the underlying, identifiable data can be disclosed. Laws and enable a user to redata set. In addition, when deregulations that address reidentify de-identified identified information is combined identifiability include: HIPAA, Common data and what with other types of identifiable Rule, Part 2. protections may information, there may be enough apply to prevent or similar data elements between the limit re-identification. two sets of information to allow a user to identify the subject. Where was the data Consider where Data may be collected in a way that The original location of data collection collected? How was and collection method may effect the allows the collector to identify the data was originally the data collected? individual, such as through an indegree to which privacy laws and collected and the person interview, or may be regulations apply to specific data. method of collection collected in a way that protects the Laws and regulations that distinguish to determine individual's identity, such as through protections based on the whether specific circumstances of collection include: an anonymous survey. requirements may HIPAA, Common Rule, Part 2. apply to your use of that information.

*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

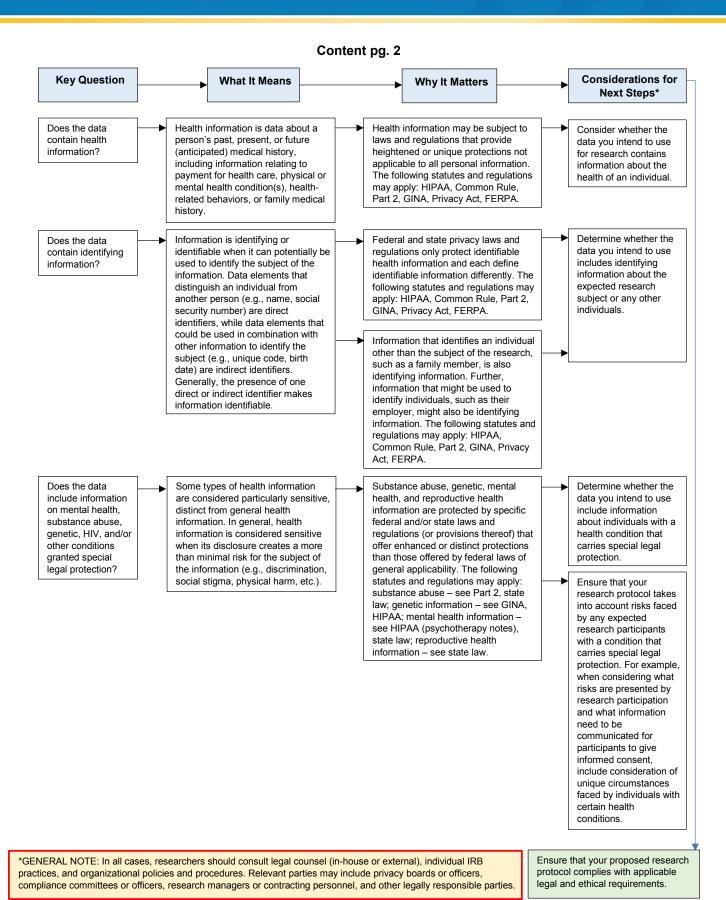
Ensure that your proposed research protocol complies with applicable legal and ethical requirements.

Data Characteristic 2: Content



Content

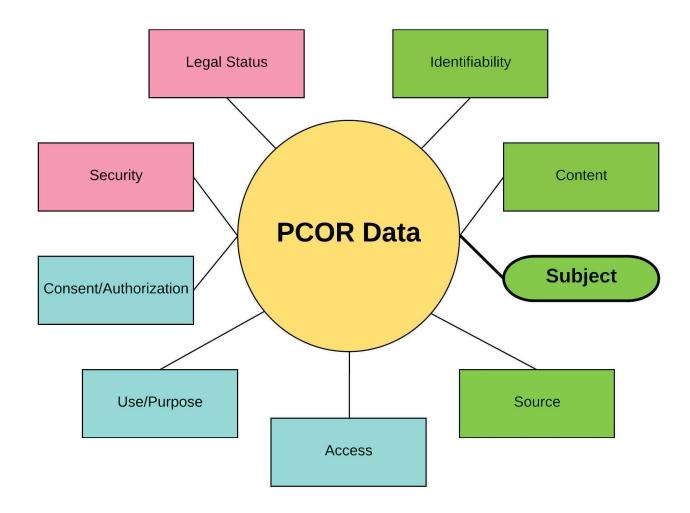
Content refers to the subject matter or substance of the data.



Legal and Ethical Architecture for PCOR Data
Chapter 4: Framework for Navigating Legal and Ethical Requirements for PCOR

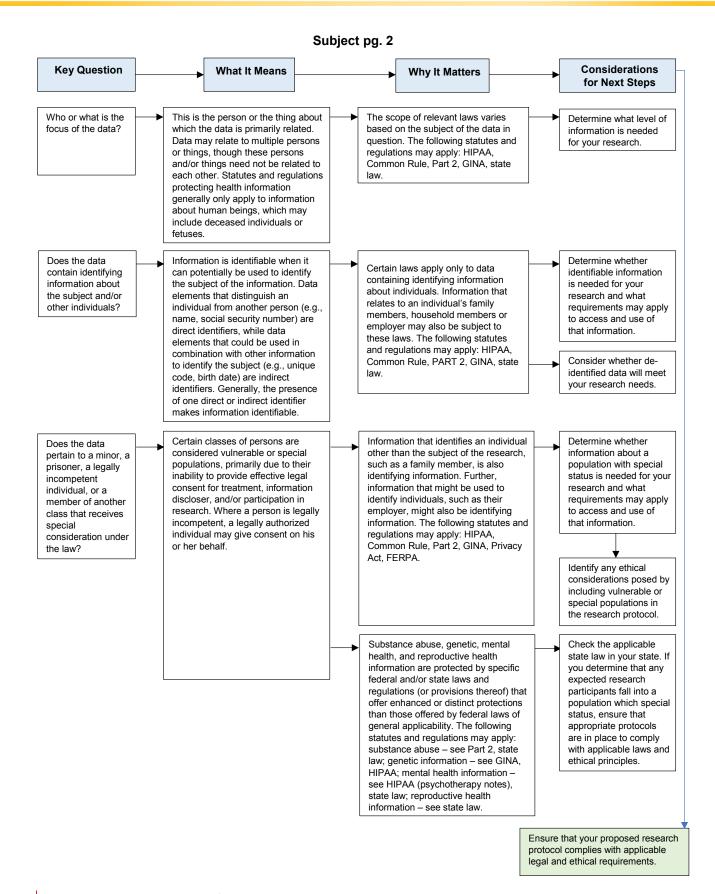
September 28, 2017

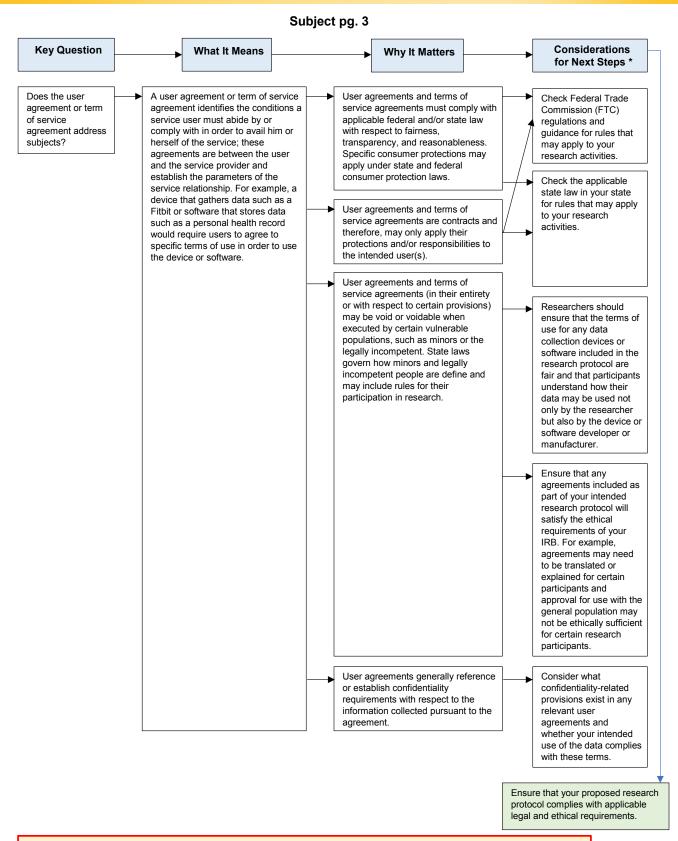
Data Characteristic 3: Subject



Subject

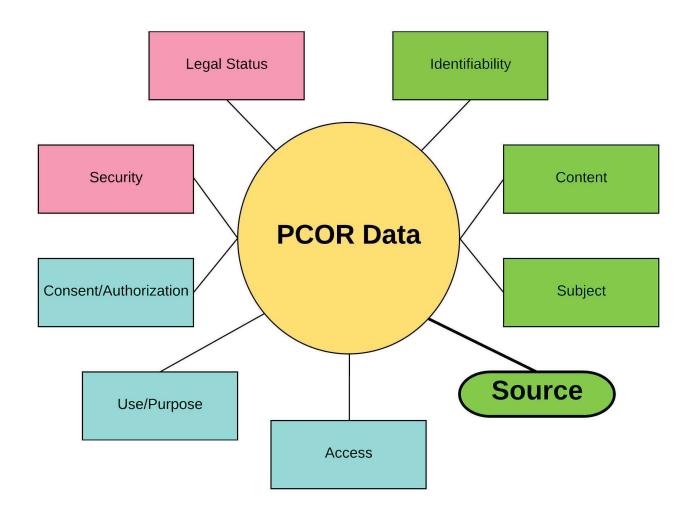
Subject refers to the person or thing that is the focus of the data.





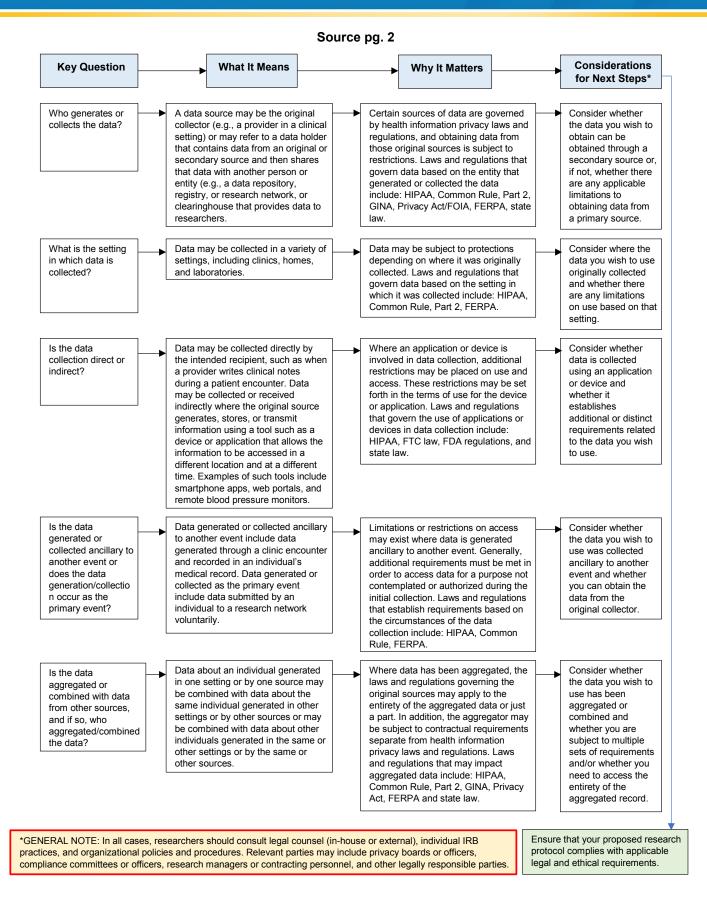
*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

Data Characteristic 4: Source

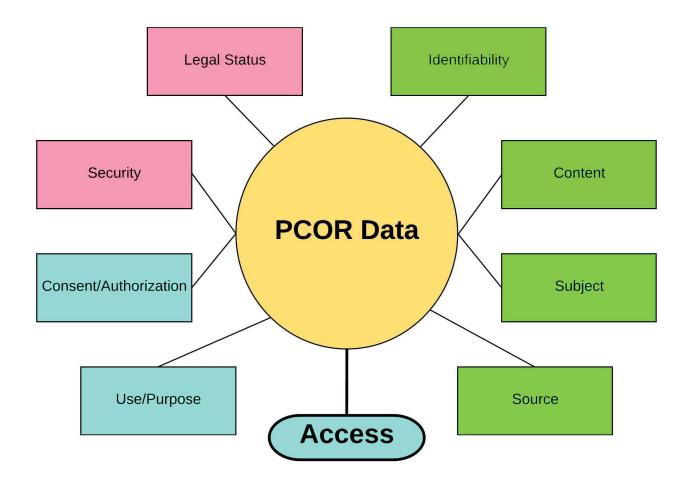


Source

Source refers to the person, entity, and/or setting in which the data originated or was collected.

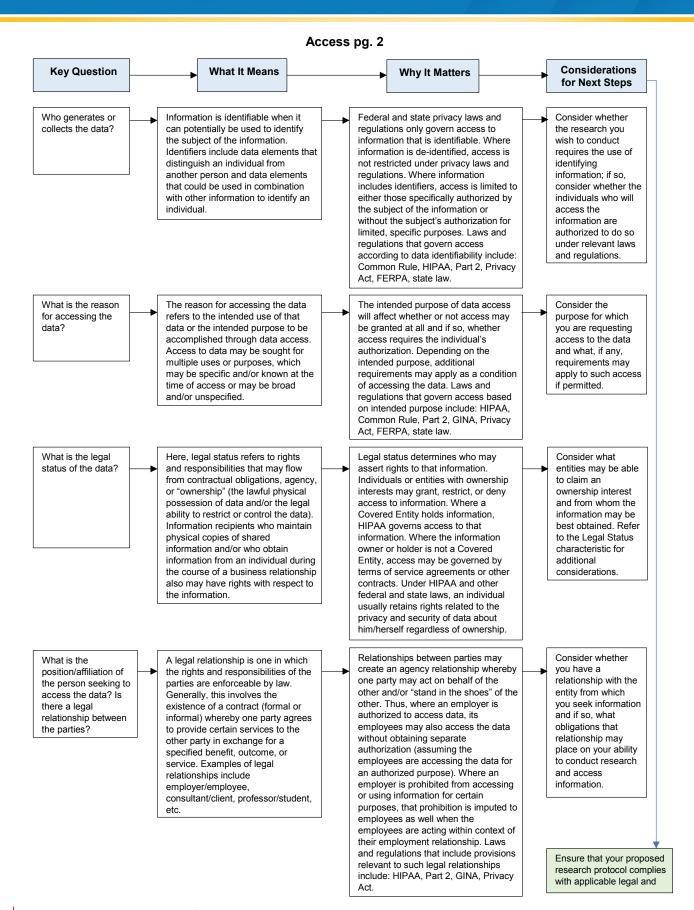


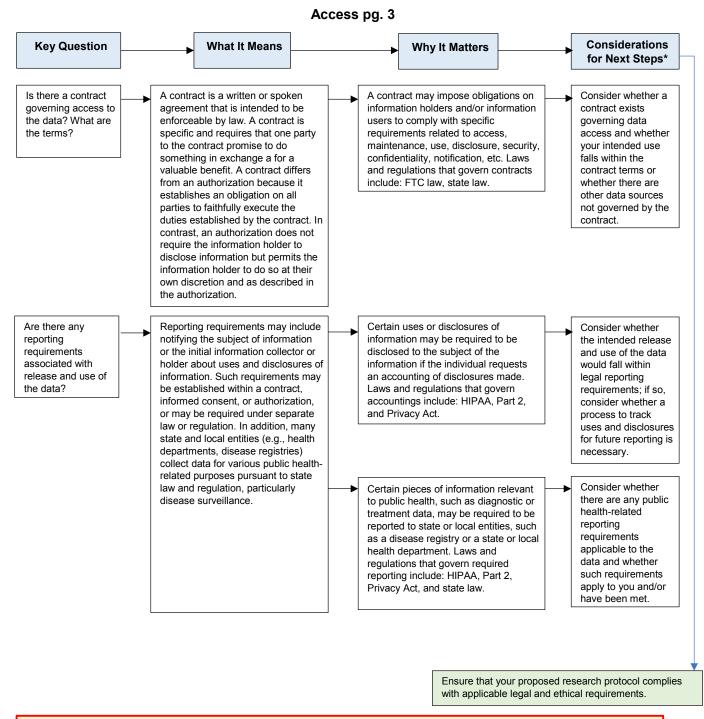
Data Characteristic 5: Access



Access

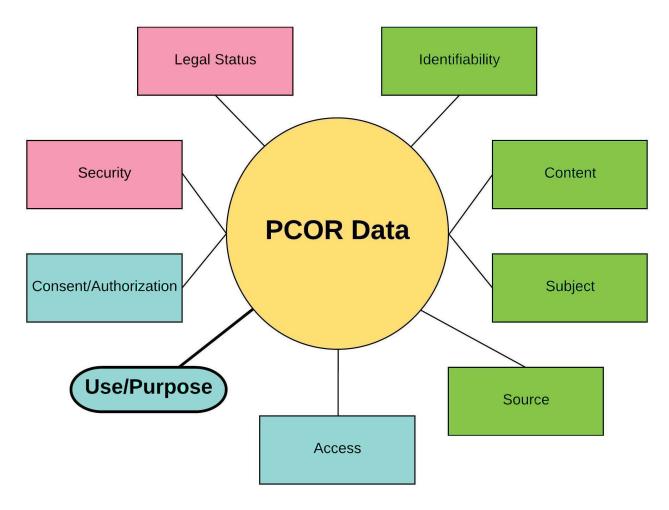
Access refers to the ability of a person or entity other than the individual subject(s) of the information to view, create, edit, or share data.





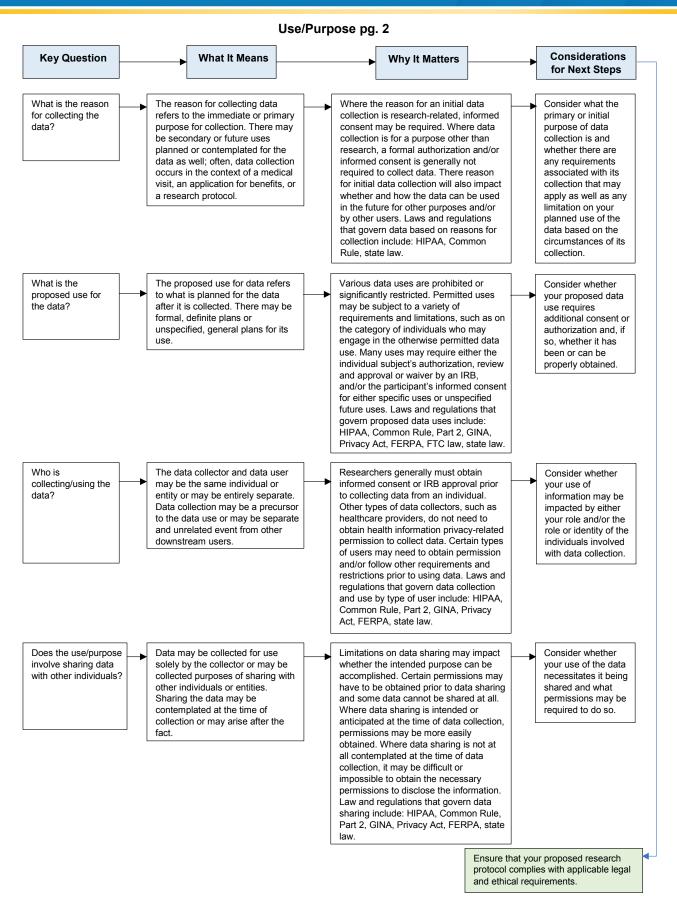
*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

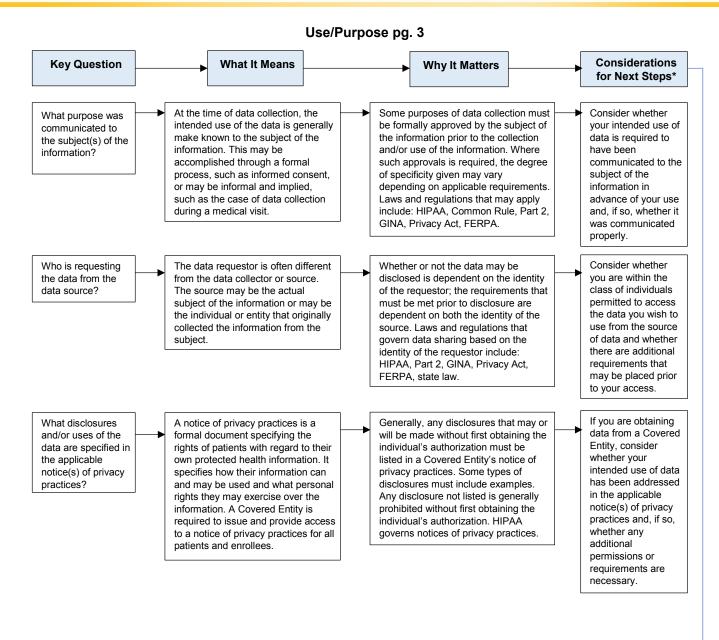
Data Characteristic 6: Use/Purpose



Use/Purpose

The intended use or purpose of the data collection will affect whether and how the data may be collected and used.

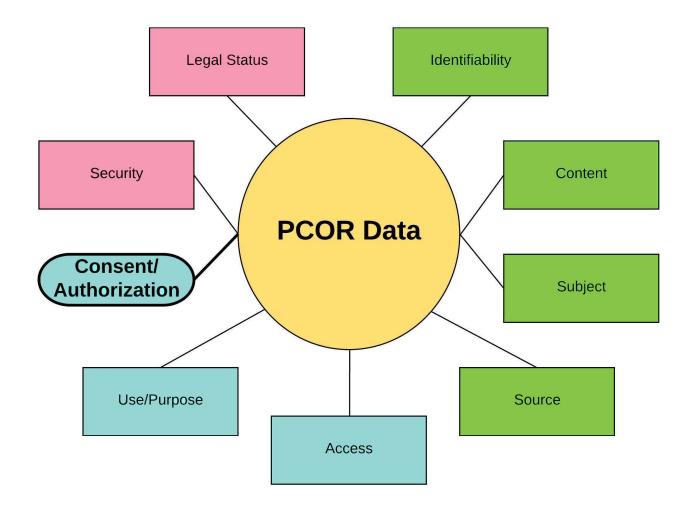




Ensure that your proposed research protocol complies with applicable legal and ethical requirements.

*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

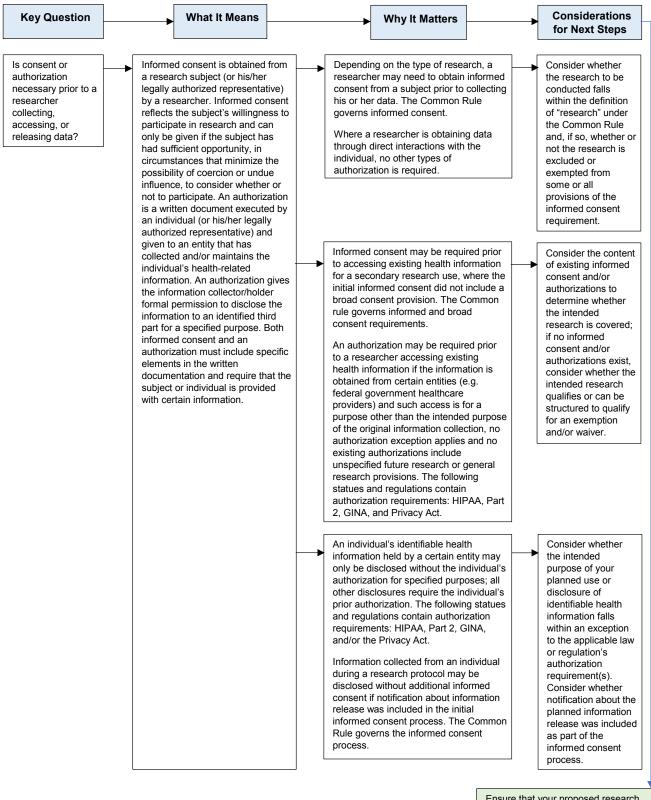
Data Characteristic 7: Consent/Authorization



Consent/Authorization

Consent/Authorization refers to the activities and documentation potentially required of researchers seeking permission to collect, use, or share data about an individual.

Consent/Authorization pg. 2



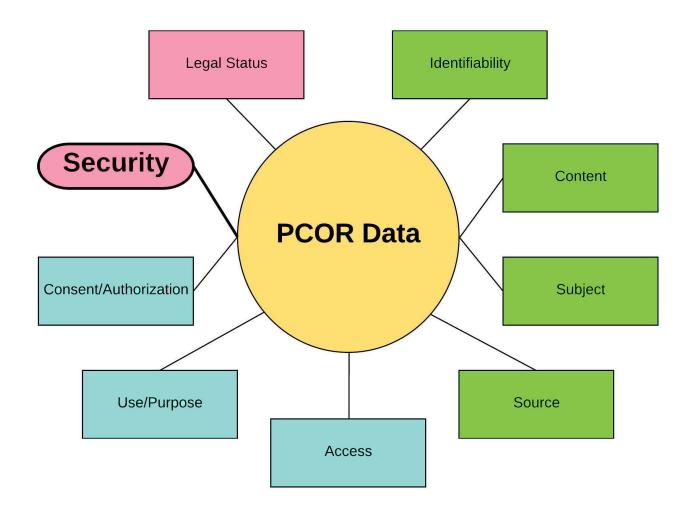
Ensure that your proposed research protocol complies with applicable legal and ethical requirements.

Consent/Authorization pg. 3 What It Means Considerations **Key Question** Why It Matters for Next Steps An Institutional Review Board Federally-supported research involving Consider whether Is the data being (IRB) is a committee formally living human participants and/or the research you collected used for a study that is subject designated to approve, oversee, and biospecimens requires IRB approval plan to conduct is review research conducted at the before research may begin unless the defined as research to Institutional Review Board (IRB) institution or research conducted at research is excluded from the definition under the Common multiple institutions that agree to use of research or exempted from the IRB Rule and, if so. approval? approval requirement. The Common whether it would fall a single-site IRB. An IRB will approve a research protocol only Rule governs IRB approval. within a Common when it meets specific requirements Rule exemption (or designed to protect subjects' health exclusion). privacy and safety. Has an IRB waived Informed consent is obtained from Consider whether the IRBs may waive or alter some or all the informed a research subject (or his/her informed consent requirements under research you plan to consent procedure legally authorized representative) certain circumstances. The Common conduct would fall applicable to partici by a researcher. Informed consent Rule governs informed consent within one of the pating in research? reflects the subject's willingness to categories eligible for procedures. participate in research and can only informed consent be given if the subject has had alteration or waiver sufficient opportunity, in and consider whether circumstances that minimize the to propose such possibility of coercion or undue waiver or alteration to influence, to consider whether or the IRB during the not to participate. review process. An authorization is a written Has an IRB waived Certain research activities may be Consider whether document executed by an individual the authorization conducted without first obtaining an the research you (or his/her personal representative) requirement authorization to access information from plan to conduct and given to an entity that has applicable to collected and/or maintains the the subject of the information if an IRB would be eligible for information has waived or altered this requirement. an authorization individual's health-related disclosure? HIPAA governs authorization waivers. alteration or waiver information. An authorization gives and consider the information collector/holder whether to seek formal permission to disclose the information to an identified third such waiver or alteration from the party for a specified purpose. Generally, an authorization is **IRB** required for all uses and disclosures of identifiable health information by a Covered Entity. An IRB can waive or alter some or all of the authorization requirements for When giving informed consent and/or an specific research activities. authorization to disclose information, the individual must be informed of his/her right to revoke consent and/or authorization at any time. If an individual has declined to Can persons withdraw An individual is legally permitted to Consider whether the continue participating in a research stop participating in a research intended research their protocol, the researcher may not continue consent/authorization? protocol, revoke an existing subjects have been to collect information about the individual. authorization to disclose his/her properly informed of Similarly, where an individual has information, and/or to have his/her their right to revoke withdrawn his/her authorization to disclose information removed from a and whether any information and/or requested removal of research dataset at any time during existing subjects his/her information from a research or after participating in a research have revoked some dataset, the researcher must comply and or all of their prior protocol may not continue to use or disclose that consent and/or information. However, prior uses or authorization. disclosures of that information are not Consider whether the covered by the individual's revocation. The research involves following laws and regulations govern the special populations. revocation consent and/or authorization: HIPAA, Common Rule, Part 2, GINA, Privacy Act, state law. Ensure that your proposed research protocol complies with applicable legal

and ethical requirements

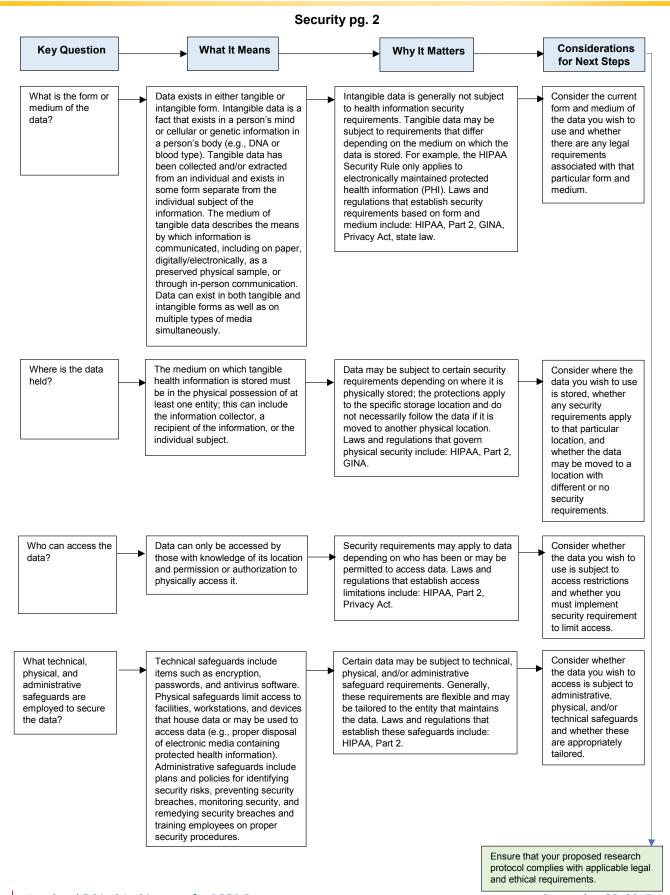
Consent/Authorization pg. 4 Considerations What It Means **Key Question** Why It Matters for Next Steps* Consider whether the Can persons opt-Opting-out of certain uses of And individual can only opt-out of out of particular information occurs where an certain uses of information where given research protocol can or should include opt-out uses for their individual declines to assent to the opportunity to do so; such information (e.g. provisions and, if so, specific uses or disclosures while opportunity is not required as part of the commercial uses)? how the opt-out simultaneously assenting to other informed consent or authorization provisions should be specific uses or disclosures. process (other than where broad consent is sought in addition to the structured and presented to the underlying consent or authorization). A researcher may wish to give an individual and managed individual the opportunity to decline for the duration of the certain uses of his/her information or research protocol. may include all uses of information as part of the entire research protocol, such that a subject either agrees to participate and allow all identified disclosures, or declines to participate at all. The following laws and regulations specifically include provisions related to structuring opt-out provisions: HIPAA. Common Rule, Part 2, state law. Where an individual lacks capacity, the Consider whether the Did an agent (e.g., Where an individual has properly intended subject of your individual cannot give legally valid parent, person with designated a third party to act on research lacks capacity consent to participate in research of medial power of his/her behalf or cannot legally act authorization to disclose information, and/or has designated a independently (i.e., lacks capacity attorney) give legally authorized due to age or mental competency), consent/authorization may only be consent or provided by his/her agent. Where an representative. an agent may provide consent to authorization? individual has designated an agent to participate in research or to act as his/her personal representative, disclose information on behalf of the agent must be treated as the the individual. individual in exercising rights related to information access and disclosure. Laws and regulations that may be implicated include HIPAA, Common Rule, Part 2, GINA, State Law. Was Conditional authorizations and In general, conditional authorizations Consider the circumstances related to consent/authorization consents exist where the individual and consents are prohibited. The laws obtaining and documenting a condition of subject of the research or and regulations that govern conditional receiving something identifiable health information is informed consent, and/or consent and authorization include: authorization to disclose else (such as medical asked to provide informed consent HIPAA, Common Rule, Part 2, GINA, information (if ant) and to participate in research and/or state law. treatment or whether there are any payment)? authorization to disclose legal or ethical obligations information in exchange for the associated with these individual receiving something circumstances unrelated from the researcher or information collector. Combination authorizations and Informed consent and authorization to Consider what Was informed consent forms are generally consent/authorization disclose information must be permissions you might documented in writing and include permissible if certain requirements are require for the research combined with certain elements. Combining these met. The combined permissions must permission for you wish to conduct and and other forms into a single be related to each other (e.g., informed something else? whether you can document may be permissible and consent to participate in a research combine any of the may mean that required elements protocol and an authorization to documents; if so, shared across both types of disclose health information to the consider the permissions need only be presented researcher for that protocol). The laws requirements applicable once (e.g., signed and dated). Other and regulations that govern conditional to each document and examples of documents that may be consent and authorization include: ensure that your merged include an acknowledgement HIPAA, Common Rule, Part 2, GINA, combined documents of receipt of notice of privacy state law. practices, consent to receive medical meets all requirements. treatment, explanation of benefits, etc. *GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB Ensure that your proposed research practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, protocol complies with applicable legal compliance committees or officers, research managers or contracting personnel, and other legally responsible and ethical requirements. parties.

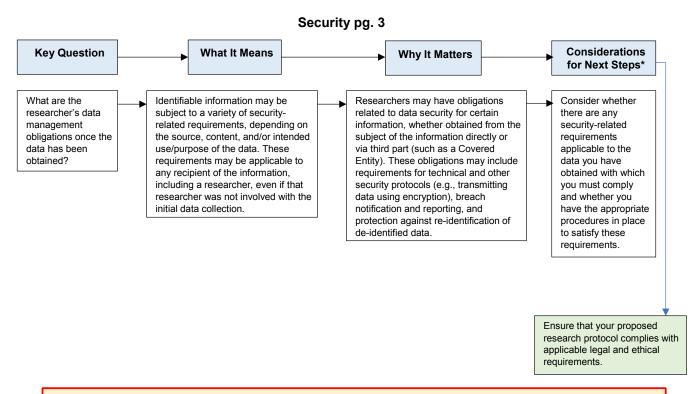
Data Characteristic 8: Security



Security

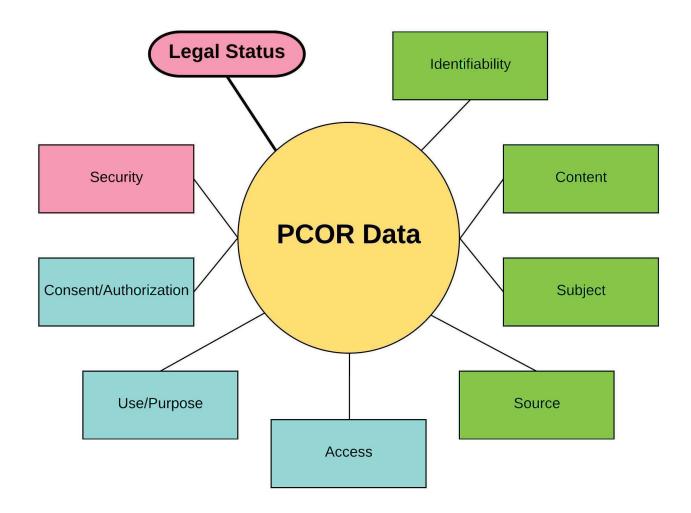
Security refers to the means by which data is protected from unauthorized use or access.





*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

Data Characteristic 9: Legal Status



Legal Status

Legal Status refers to rights and responsibilities related to the data that may be triggered by ownership rights, agency principles, and/or contractual obligations.

Legal Status pg. 2 Considerations **Key Question** What It Means Why It Matters for Next Steps* Consider what entities Who owns the Data ownership generally refers to Data ownership gives the owner the the lawful physical possession of right to grant, restrict, or deny access to may be able to claim an data? ownership interest in the data and/or the legal ability to information. Where a Covered Entity is restrict or control the data. the owner of information, HIPAA also data of interest. Then consider whether the Regardless of ownership, governs disclosure of the data (and individual subjects of data may other requirements relating to its use) owner is a Covered maintain certain rights related to may be determined by a contract, state Entity or whether a nonthe privacy and security of their law, or property law (including Covered Entity can data. Multiple parties may have intellectual property law). Ownership of claim an ownership stake and from which ownership rights to the same individual identifiable information, information. especially genetic information such as the information may be more easily obtained. DNA, may be restricted by ethical principles and state and federal law may restrict certain uses, such as selling. Laws and regulations that may be implicated include HIPAA, GINA, state law, and federal intellectual property law. Are there contracts Examples of contracts that may Access to data (and other requirements Consider what in place that govern govern data access, use, and relating to its use) may be determined obligations may be exchange include a funding by a contract between the data seeker how the parties to required by any the contract or their agreement between a grant funder and data owner or holder. State law contracts in place, (including common law) governs agents may use the and a grant recipient, a terms of including how data must data? service agreement between a construction and enforcement of be handled and how it database vendor and a researcher may be shared. contracts. purchasing access to the database, a contract between an insurer and a healthcare provider, and an employment contract between a researcher and a healthcare organization. What is the Under the legal principle of Legal relationships may give a Consider the position of position/affiliation of researcher a right to access data, such the parties seeking and agency, a principal party grants as when the researcher's employer has the person seeking authority for another party, the holding data and whether access to the data? agent, to act on the principal's purchased access to data or where the existing relationships researcher's organization is part of a Is there a legal behalf in dealings with third affect rights with respect relationship between parties. Employees are generally corporate entity with the institution that to data access. the parties (e.g., agents of their employers. Where holds the data. State law (including employment)? the researcher is an agent of common law) governs legal relationships that create agency. another party, such as a healthcare provider, the researcher has the rights and obligations of the healthcare provider. Some state laws, such as consumer Some state laws may confer rights that Consider what state laws Does any state law apply regardless of agreements protection and patient privacy laws, grant ownership may apply to the data between parties. For example, New rights or rights to may confer rights and you are seeking to responsibilities with respect to Hampshire grants patients' ownership restrict access? access rights over their health information. A access to data or data held by patient may exert this right to prevent researchers. their health information from being included in a research database. Some state laws may require information to be made available to certain parties, such as patients, even if they exist in research databases, such as registries. or are held by researchers.

*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

Ensure that your proposed research protocol complies with applicable legal and ethical requirements.