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

**INTRODUCTION** ............................................................................................................... 1

**PCOR FRAMEWORK** ....................................................................................................... 1

- 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 ............................................................................... 26
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.
Identifiability

Identifiability refers to the ability to link information to particular individuals.
Key Question | What It Means | Why It Matters | Considerations for Next Steps*
--- | --- | --- | ---
What information does the data contain? Does this information directly identify individuals? | Identifying data elements are those that allow the user to link the information to the individual subject of the information. These elements can be direct identifiers (e.g., an individual's name, social security number) or can be indirect identifiers (e.g., information that, when taken as a whole or when combined with other available information, can be used to identify an individual). | Health-related data that contains any identifying information may be subject to the health information privacy framework. Even a data set stripped of most direct identifiers such as a limited data set, is considered identifiable because one or more direct identifiers are present. Laws and regulations that define identifiability and protect certain types of identifiable information include: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA state law. | Consider whether the data you wish to use for your research must be in identifiable form and what requirements apply to your use of that data.

Has the data been de-identified? If so, how? | Information that was once identifiable but has been stripped of any elements that directly identify the individual or could be used to identify the individual is considered "de-identified." The process by which de-identification occurs is relevant to determining whether or not information meets applicable definitions of "de-identified." | De-identified data is generally not subject to the health information privacy framework. In general, de-identified data has either been stripped of specific identifying elements or has been deemed "de-identified" by an expert. Laws and regulations that define de-identified data and set forth requirements for it include: HIPAA, Common Rule, Part 2, state law. | Consider whether the data you wish to use for your research has been de-identified and whether this process meets applicable legal standards.

Can the data be re-identified when combined with data from another source? | Data that has been stripped of all identifying information may include a key or code that allows certain users to link the de-identified information back to the underlying, identifiable data set. In addition, when de-identified information is combined with other types of identifiable information, there may be enough similar data elements between the two sets of information to allow a user to identify the subject. | If a user knows that de-identified data could still be used to identify the individual in some way, there may be limitations on how and to whom the data can be disclosed. Laws and regulations that address re-identifiability include: HIPAA, Common Rule, Part 2. | Consider whether there is other available information or a key that would enable a user to re-identify de-identified data and what protections may apply to prevent or limit re-identification.

Where was the data collected? How was the data collected? | Data may be collected in a way that allows the collector to identify the individual, such as through an in-person interview, or may be collected in a way that protects the individual's identity, such as through an anonymous survey. | The original location of data collection and collection method may effect the degree to which privacy laws and regulations apply to specific data. Laws and regulations that distinguish protections based on the circumstances of collection include: HIPAA, Common Rule, Part 2. | Consider where data was originally collected and the method of collection to determine whether specific requirements may apply to your use of that information.

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.
Content

Content refers to the subject matter or substance of the data.
**Key Question**

Does the data contain health information?

**What It Means**

Health information is data about a person’s past, present, or future (anticipated) medical history, including information relating to payment for health care, physical or mental health condition(s), health-related behaviors, or family medical history.

**Why It Matters**

Health information may be subject to laws and regulations that provide heightened or unique protections not applicable to all personal information. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA.

**Considerations for Next Steps***

Consider whether the data you intend to use for research contains information about the health of an individual.

---

Does the data contain identifying information?

**What It Means**

Information is identifying or identifiable when it can potentially be used to identify the subject of the information. Data elements that distinguish an individual from another person (e.g., name, social security number) are direct identifiers, while data elements that could be used in combination with other information to identify the subject (e.g., unique code, birth date) are indirect identifiers. Generally, the presence of one direct or indirect identifier makes information identifiable.

**Why It Matters**

Federal and state privacy laws and regulations only protect identifiable health information and each define identifiable information differently. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA.

**Considerations for Next Steps***

Determine whether the data you intend to use includes identifying information about the expected research subject or any other individuals.

---

Does the data include information on mental health, substance abuse, genetic, HIV, and/or other conditions granted special legal protection?

**What It Means**

Some types of health information are considered particularly sensitive, distinct from general health information. In general, health information is considered sensitive when its disclosure creates a more than minimal risk for the subject of the information (e.g., discrimination, social stigma, physical harm, etc.).

**Why It Matters**

Substance abuse, genetic, mental health, and reproductive health information are protected by specific federal and/or state laws and regulations (or provisions thereof) that offer enhanced or distinct protections than those offered by federal laws of general applicability. The following statutes and regulations may apply: substance abuse – see Part 2, state law; genetic information – see GINA, HIPAA; mental health information – see HIPAA (psychotherapy notes), state law; reproductive health information – see state law.

**Considerations for Next Steps***

Determine whether the data you intend to use include information about individuals with a health condition that carries special legal protection. Ensure that your proposed research protocol takes into account risks faced by any expected research participants with a condition that carries special legal protection. For example, when considering what risks are presented by research participation and what information need to be communicated for participants to give informed consent, include consideration of unique circumstances faced by individuals with certain health conditions.

---

*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 research protocol complies with applicable legal and ethical requirements.
Data Characteristic 3: Subject

Subject

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

Who or what is the focus of the data?

**What It Means**

This is the person or the thing about which the data is primarily related. Data may relate to multiple persons or things, though these persons and/or things need not be related to each other. Statutes and regulations protecting health information generally only apply to information about human beings, which may include deceased individuals or fetuses.

**Why It Matters**

The scope of relevant laws varies based on the subject of the data in question. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, state law.

**Considerations for Next Steps**

Determine what level of information is needed for your research.

---

**Key Question**

Does the data contain identifying information about the subject and/or other individuals?

**What It Means**

Information is identifiable when it can potentially be used to identify the subject of the information. Data elements that distinguish an individual from another person (e.g., name, social security number) are direct identifiers, while data elements that could be used in combination with other information to identify the subject (e.g., unique code, birth date) are indirect identifiers. Generally, the presence of one direct or indirect identifier makes information identifiable.

**Why It Matters**

Certain laws apply only to data containing identifying information about individuals. Information that relates to an individual’s family members, household members or employer may also be subject to these laws. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, state law.

**Considerations for Next Steps**

Determine whether identifiable information is needed for your research and what requirements may apply to access and use of that information.

---

**Key Question**

Does the data pertain to a minor, a prisoner, a legally incompetent individual, or a member of another class that receives special consideration under the law?

**What It Means**

Certain classes of persons are considered vulnerable or special populations, primarily due to their inability to provide effective legal consent for treatment, information disclosure, and/or participation in research. Where a person is legally incompetent, a legally authorized individual may give consent on his or her behalf.

**Why It Matters**

Information that identifies an individual other than the subject of the research, such as a family member, is also identifying information. Further, information that might be used to identify individuals, such as their employer, might also be identifying information. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA.

**Considerations for Next Steps**

Determine whether information about a population with special status is needed for your research and what requirements may apply to access and use of that information.

---

**Key Question**

Substance abuse, genetic, mental health, and reproductive health information are protected by specific federal and/or state laws and regulations (or provisions thereof) that offer enhanced or distinct protections than those offered by federal laws of general applicability. The following statutes and regulations may apply: substance abuse – see Part 2, state law; genetic information – see GINA, HIPAA; mental health information – see HIPAA (psychotherapy notes), state law; reproductive health information – see state law.

**Considerations for Next Steps**

Identify any ethical considerations posed by including vulnerable or special populations in the research protocol.

Check the applicable state law in your state. If you determine that any expected research participants fall into a population which special status, ensure that appropriate protocols are in place to comply with applicable laws and ethical principles.

---

Ensure that your proposed research protocol complies with applicable legal and ethical requirements.
**Key Question**
Does the user agreement or term of service agreement address subjects?

**What It Means**
A user agreement or term of service agreement identifies the conditions a service user must abide by or comply with in order to avail him or herself of the service; these agreements are between the user and the service provider and establish the parameters of the service relationship. For example, a device that gathers data such as a Fitbit or software that stores data such as a personal health record would require users to agree to specific terms of use in order to use the device or software.

**Why It Matters**
User agreements and terms of service agreements must comply with applicable federal and/or state law with respect to fairness, transparency, and reasonableness. Specific consumer protections may apply under state and federal consumer protection laws.

User agreements and terms of service agreements are contracts and therefore, may only apply their protections and/or responsibilities to the intended user(s).

User agreements and terms of service agreements (in their entirety or with respect to certain provisions) may be void or voidable when executed by certain vulnerable populations, such as minors or the legally incompetent. State laws govern how minors and legally incompetent people are define and may include rules for their participation in research.

User agreements generally reference or establish confidentiality requirements with respect to the information collected pursuant to the agreement.

**Considerations for Next Steps**

Check Federal Trade Commission (FTC) regulations and guidance for rules that may apply to your research activities.

Check the applicable state law in your state for rules that may apply to your research activities.

Researchers should ensure that the terms of use for any data collection devices or software included in the research protocol are fair and that participants understand how their data may be used not only by the researcher but also by the device or software developer or manufacturer.

Ensure that any agreements included as part of your intended research protocol will satisfy the ethical requirements of your IRB. For example, agreements may need to be translated or explained for certain participants and approval for use with the general population may not be ethically sufficient for certain research participants.

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 4: Source

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

Who generates or collects the data?

**What It Means**

A data source may be the original collector (e.g., a provider in a clinical setting) or may refer to a data holder that contains data from an original or secondary source and then shares that data with another person or entity (e.g., a data repository, registry, or research network, or clearinghouse that provides data to researchers).

**Why It Matters**

Certain sources of data are governed by health information privacy laws and regulations, and obtaining data from those original sources is subject to restrictions. Laws and regulations that govern data based on the entity that generated or collected the data include: HIPAA, Common Rule, Part 2, GINA, Privacy Act/FOIA, FERPA, state law.

**Considerations for Next Steps**

Consider whether the data you wish to obtain can be obtained through a secondary source or, if not, whether there are any applicable limitations to obtaining data from a primary source.

---

**Key Question**

What is the setting in which data is collected?

**What It Means**

Data may be collected in a variety of settings, including clinics, homes, and laboratories.

**Why It Matters**

Data may be subject to protections depending on where it was originally collected. Laws and regulations that govern data based on the setting in which it was collected include: HIPAA, Common Rule, Part 2, FERPA.

**Considerations for Next Steps**

Consider where the data you wish to use originally collected and whether there are any limitations on use based on that setting.

---

**Key Question**

Is the data collection direct or indirect?

**What It Means**

Data may be collected directly by the intended recipient, such as when a provider writes clinical notes during a patient encounter. Data may be collected or received indirectly where the original source generates, stores, or transmits information using a tool such as a device or application that allows the information to be accessed in a different location and at a different time. Examples of such tools include smartphone apps, web portals, and remote blood pressure monitors.

**Why It Matters**

Where an application or device is involved in data collection, additional restrictions may be placed on use and access. These restrictions may be set forth in the terms of use for the device or application. Laws and regulations that govern the use of applications or devices in data collection include: HIPAA, FTC law, FDA regulations, and state law.

**Considerations for Next Steps**

Consider whether data is collected using an application or device and whether it establishes additional or distinct requirements related to the data you wish to use.

---

**Key Question**

Is the data generated or collected ancillary to another event or does the data generation/collectio n occur as the primary event?

**What It Means**

Data generated or collected ancillary to another event include data generated through a clinic encounter and recorded in an individual’s medical record. Data generated or collected as the primary event include data submitted by an individual to a research network voluntarily.

**Why It Matters**

Limitations or restrictions on access may exist where data is generated ancillary to another event. Generally, additional requirements must be met in order to access data for a purpose not contemplated or authorized during the initial collection. Laws and regulations that establish requirements based on the circumstances of the data collection include: HIPAA, Common Rule, FERPA.

**Considerations for Next Steps**

Consider whether the data you wish to use was collected ancillary to another event and whether you can obtain the data from the original collector.

---

**Key Question**

Is the data aggregated or combined with data from other sources, and if so, who aggregated/combined the data?

**What It Means**

Data about an individual generated in one setting or by one source may be combined with data about the same individual generated in other settings or by other sources or may be combined with data about other individuals generated in the same or other settings or by the same or other sources.

**Why It Matters**

Where data has been aggregated, the laws and regulations governing the original sources may apply to the entirety of the aggregated data or just a part. In addition, the aggregator may be subject to contractual requirements separate from health information privacy laws and regulations. Laws and regulations that may impact aggregated data include: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA and state law.

**Considerations for Next Steps**

Consider whether the data you wish to use has been aggregated or combined and whether you are subject to multiple sets of requirements and/or whether you need to access the entirety of the aggregated record.

---

**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.
**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.
Key Question: What is the reason for accessing the data?

What It Means: The reason for accessing the data refers to the intended use of that data or the intended purpose to be accomplished through data access. Access to data may be sought for multiple uses or purposes, which may be specific and/or known at the time of access or may be broad and/or unspecified.

Why It Matters: The intended purpose of data access will affect whether or not access may be granted at all and if so, whether access requires the individual’s authorization. Depending on the intended purpose, additional requirements may apply as a condition of accessing the data. Laws and regulations that govern access based on intended purpose include: HIPAA, Common Rule, Part 2, Privacy Act, FERPA, state law.

Considerations for Next Steps: Consider the purpose for which you are requesting access to the data and what, if any, requirements may apply to such access if permitted.

Key Question: What is the legal status of the data?

What It Means: Here, legal status refers to rights and responsibilities that may flow from contractual obligations, agency, or ownership (the lawful physical possession of data and/or the legal ability to restrict or control the data). Information recipients who maintain physical copies of shared information and/or who obtain information from an individual during the course of a business relationship also may have rights with respect to the information.

Why It Matters: Legal status determines who may assert rights to that information. Individuals or entities with ownership interests may grant, restrict, or deny access to information. Where a Covered Entity holds information, HIPAA governs access to that information. Where the information owner or holder is not a Covered Entity, access may be governed by terms of service agreements or other contracts. Under HIPAA and other federal and state laws, an individual usually retains rights related to the privacy and security of data about him/herself regardless of ownership.

Considerations for Next Steps: Consider whether entities may be able to claim an ownership interest and from whom the information may be best obtained. Refer to the Legal Status characteristic for additional considerations.

Key Question: What is the position/affiliation of the person seeking to access the data? Is there a legal relationship between the parties?

What It Means: A legal relationship is one in which the rights and responsibilities of the parties are enforceable by law. Generally, this involves the existence of a contract (formal or informal) whereby one party agrees to provide certain services to the other party in exchange for a specified benefit, outcome, or service. Examples of legal relationships include employer/employee, consultant/client, professor/student, etc.

Why It Matters: Relationships between parties may create an agency relationship whereby one party may act on behalf of the other and/or “stand in the shoes” of the other. Thus, where an employer is authorized to access data, its employees may also access the data without obtaining separate authorization (assuming the employees are accessing the data for an authorized purpose). Where an employer is prohibited from accessing or using information for certain purposes, that prohibition is imputed to employees as well when the employees are acting within context of their employment relationship. Laws and regulations that include provisions relevant to such legal relationships include: HIPAA, Part 2, GINA, Privacy Act.

Considerations for Next Steps: Consider whether you have a relationship with the entity from which you seek information and if so, what obligations that relationship may place on your ability to conduct research and access information.

Considerations for Next Steps: Ensure that your proposed research protocol complies with applicable legal and...
Key Question | What It Means | Why It Matters | Considerations for Next Steps*
--- | --- | --- | ---
Is there a contract governing access to the data? What are the terms? | A contract is a written or spoken agreement that is intended to be enforceable by law. A contract is specific and requires that one party to the contract promise to do something in exchange for a valuable benefit. A contract differs from an authorization because it establishes an obligation on all parties to faithfully execute the duties established by the contract. In contrast, an authorization does not require the information holder to disclose information but permits the information holder to do so at their own discretion and as described in the authorization. | A contract may impose obligations on information holders and/or information users to comply with specific requirements related to access, maintenance, use, disclosure, security, confidentiality, notification, etc. Laws and regulations that govern contracts include: FTC law, state law. | Consider whether a contract exists governing data access and whether your intended use falls within the contract terms or whether there are other data sources not governed by the contract. |
Are there any reporting requirements associated with release and use of the data? | Reporting requirements may include notifying the subject of information or the initial information collector or holder about uses and disclosures of information. Such requirements may be established within a contract, informed consent, or authorization, or may be required under separate law or regulation. In addition, many state and local entities (e.g., health departments, disease registries) collect data for various public health-related purposes pursuant to state law and regulation, particularly disease surveillance. | Certain uses or disclosures of information may be required to be disclosed to the subject of the information if the individual requests an accounting of disclosures made. Laws and regulations that govern accountings include: HIPAA, Part 2, and Privacy Act. | Consider whether the intended release and use of the data would fall within legal reporting requirements; if so, consider whether a process to track uses and disclosures for future reporting is necessary. |
| | | Certain pieces of information relevant to public health, such as diagnostic or treatment data, may be required to be reported to state or local entities, such as a disease registry or a state or local health department. Laws and regulations that govern required reporting include: HIPAA, Part 2, Privacy Act, and state law. | Consider whether there are any public health-related reporting requirements applicable to the data and whether such requirements apply to you and/or have been met. |

*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 6: Use/Purpose

The intended use or purpose of the data collection will affect whether and how the data may be collected and used.
Use/Purpose pg. 2

Key Question  What It Means  Why It Matters  Considerations for Next Steps

What is the reason for collecting the data?

The reason for collecting data refers to the immediate or primary purpose for collection. There may be secondary or future uses planned or contemplated for the data as well; often, data collection occurs in the context of a medical visit, an application for benefits, or a research protocol.

Where the reason for an initial data collection is research-related, informed consent may be required. Where data collection is for a purpose other than research, a formal authorization and/or informed consent is generally not required to collect data. There reason for initial data collection will also impact whether and how the data can be used in the future for other purposes and/or by other users. Laws and regulations that govern data based on reasons for collection include: HIPAA, Common Rule, state law.

Consider what the primary or initial purpose of data collection is and whether there are any requirements associated with its collection that may apply as well as any limitation on your planned use of the data based on the circumstances of its collection.

What is the proposed use for the data?

The proposed use for data refers to what is planned for the data after it is collected. There may be formal, definite plans or unspecified, general plans for its use.

Various data uses are prohibited or significantly restricted. Permitted uses may be subject to a variety of requirements and limitations, such as on the category of individuals who may engage in the otherwise permitted data use. Many uses may require either the individual subject’s authorization, review and approval or waiver by an IRB, and/or the participant’s informed consent for either specific uses or unspecified future uses. Laws and regulations that govern proposed data uses include: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA, FTC law, state law.

Consider whether your proposed data use requires additional consent or authorization and, if so, whether it has been or can be properly obtained.

Who is collecting/using the data?

The data collector and data user may be the same individual or entity or may be entirely separate. Data collection may be a precursor to the data use or may be separate and unrelated event from other downstream users.

Researchers generally must obtain informed consent or IRB approval prior to collecting data from an individual. Other types of data collectors, such as healthcare providers, do not need to obtain health information privacy-related permission to collect data. Certain types of users may need to obtain permission and/or follow other requirements and restrictions prior to using data. Laws and regulations that govern data collection and use by type of user include: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA, state law.

Consider whether your use of information may be impacted by either your role and/or the role or identity of the individual involved with data collection.

Does the use/purpose involve sharing data with other individuals?

Data may be collected for use solely by the collector or may be collected purposes of sharing with other individuals or entities. Sharing the data may be contemplated at the time of collection or may arise after the fact.

Limitations on data sharing may impact whether the intended purpose can be accomplished. Certain permissions may have to be obtained prior to data sharing and some data cannot be shared at all. Where data sharing is intended or anticipated at the time of data collection, permissions may be more easily obtained. Where data sharing is not at all contemplated at the time of data collection, it may be difficult or impossible to obtain the necessary permissions to disclose the information. Law and regulations that govern data sharing include: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA, state law.

Consider whether your use of the data necessitates it being shared and what permissions may be required to do so.

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

What purpose was communicated to the subject(s) of the information?

**What It Means**

At the time of data collection, the intended use of the data is generally made known to the subject of the information. This may be accomplished through a formal process, such as informed consent, or may be informal and implied, such as the case of data collection during a medical visit.

**Why It Matters**

Some purposes of data collection must be formally approved by the subject of the information prior to the collection and/or use of the information. Where such approvals are required, the degree of specificity given may vary depending on applicable requirements. Laws and regulations that may apply include: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA.

**Considerations for Next Steps**

Consider whether your intended use of data is required to have been communicated to the subject of the information in advance of your use and, if so, whether it was communicated properly.

**Who is requesting the data from the data source?**

The data requestor is often different from the data collector or source. The source may be the actual subject of the information or may be the individual or entity that originally collected the information from the subject.

**What disclosures and/or uses of the data are specified in the applicable notice(s) of privacy practices?**

A notice of privacy practices is a formal document specifying the rights of patients with regard to their own protected health information. It specifies how their information can and may be used and what personal rights they may exercise over the information. A Covered Entity is required to issue and provide access to a notice of privacy practices for all patients and enrollees.

**Why It Matters**

Generally, any disclosures that may or will be made without first obtaining the individual’s authorization must be listed in a Covered Entity’s notice of privacy practices. Some types of disclosures must include examples. Any disclosure not listed is generally prohibited without first obtaining the individual’s authorization. HIPAA governs notices of privacy practices.

**Considerations for Next Steps**

If you are obtaining data from a Covered Entity, consider whether your intended use of data has been addressed in the applicable notice(s) of privacy practices and, if so, whether any additional permissions or requirements are necessary.

---

*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.*
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

Key Question: Is consent or authorization necessary prior to a researcher collecting, accessing, or releasing data?

What It Means:
- Informed consent is obtained from a research subject (or his/her legally authorized representative) by a researcher. Informed consent reflects the subject’s willingness to participate in research and can only be given if the subject has had sufficient opportunity, in circumstances that minimize the possibility of coercion or undue influence, to consider whether or not to participate. An authorization is a written document executed by an individual (or his/her legally authorized representative) and given to an entity that has collected and/or maintains the individual’s health-related information. An authorization gives the information collector/holder formal permission to disclose the information to an identified third party for a specified purpose. Both informed consent and an authorization must include specific elements in the written documentation and require that the subject or individual is provided with certain information.

Why It Matters:
- Depending on the type of research, a researcher may need to obtain informed consent from a subject prior to collecting his or her data. The Common Rule governs informed consent. Where a researcher is obtaining data through direct interactions with the individual, no other types of authorization is required.
- Informed consent may be required prior to accessing existing health information for a secondary research use, where the initial informed consent did not include a broad consent provision. The Common rule governs informed and broad consent requirements.
- An authorization may be required prior to a researcher accessing existing health information if the information is obtained from certain entities (e.g. federal government healthcare providers) and such access is for a purpose other than the intended purpose of the original information collection, no authorization exception applies and no existing authorizations include unspecified future research or general research provisions. The following statues and regulations contain authorization requirements: HIPAA, Part 2, GINA, and Privacy Act.
- An individual’s identifiable health information held by a certain entity may only be disclosed without the individual’s authorization for specified purposes; all other disclosures require the individual’s prior authorization. The following statues and regulations contain authorization requirements: HIPAA, Part 2, GINA, and/or the Privacy Act.
- Information collected from an individual during a research protocol may be disclosed without additional informed consent if notification about information release was included in the initial informed consent process. The Common Rule governs the informed consent process.

Considerations for Next Steps:
- Consider whether the research to be conducted falls within the definition of “research” under the Common Rule and, if so, whether or not the research is excluded or exempted from some or all provisions of the informed consent requirement.
- Consider whether the research to be conducted falls within the definition of “research” under the Common Rule and, if so, whether or not the research is excluded or exempted from some or all provisions of the informed consent requirement.
- Consider the content of existing informed consent and/or authorizations to determine whether the intended research is covered; if no informed consent and/or authorizations exist, consider whether the intended research qualifies or can be structured to qualify for an exemption and/or waiver.
- Consider whether the research to be conducted falls within the definition of “research” under the Common Rule and, if so, whether or not the research is excluded or exempted from some or all provisions of the informed consent requirement.
- Consider the intended purpose of your planned use or disclosure of identifiable health information falls within an exception to the applicable law or regulation’s authorization requirement(s). Consider whether notification about the planned information release was included as part of the informed consent process.

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

Ensure that your proposed research protocol complies with applicable legal and ethical requirements.
**Consent/Authorization pg. 4**

**Key Question**

- Can persons opt-out of particular uses for their information (e.g., commercial uses)?
- Was consent/authorization a condition of receiving something else (such as medical treatment or payment)?
- Was consent/authorization combined with permission for something else?

**What It Means**

- Opting-out of certain uses of information occurs where an individual declines to consent to specific uses or disclosures while simultaneously assenting to other specific uses or disclosures.
- Conditional authorizations and consents exist where the individual subject of the research or identifiable health information is asked to provide informed consent to participate in research and/or authorization to disclose information in exchange for the individual receiving something unrelated from the researcher or information collector.
- Informed consent and authorization to disclose information must be documented in writing and include certain elements. Combining these and other forms into a single document may be permissible and mean that required elements shared across both types of permissions need only be presented once (e.g., signed and dated). Other examples of documents that may be merged include an acknowledgment of receipt of notice of privacy practices, consent to receive medical treatment, explanation of benefits, etc.

**Why It Matters**

- And individual can only opt-out of certain uses of information where given the opportunity to do so; such opportunity is not required as part of the informed consent or authorization process (other than where broad consent is sought in addition to the underlying consent or authorization). A researcher may wish to give an individual the opportunity to decline certain uses of his/her information or 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.
- In general, conditional authorizations and consents are prohibited. The laws and regulations that govern conditional consent and authorization include: HIPAA, Common Rule, Part 2, GINA, state law.
- Combination authorizations and informed consent forms are generally permissible if certain requirements are met. The combined permissions must be related to each other (e.g., informed consent to participate in a research protocol and an authorization to disclose health information to the researcher for that protocol). The laws and regulations that govern conditional consent and authorization include: HIPAA, Common Rule, Part 2, GINA, state law.

**Considerations for Next Steps**

- Consider whether the research protocol can or should include opt-out provisions and, if so, how the opt-out provisions should be structured and presented to the individual and managed for the duration of the research protocol.
- Consider the circumstances related to obtaining and documenting informed consent, and/or authorization to disclose information (if any) and whether there are any legal or ethical obligations associated with these circumstances.
- Consider what permissions you might require for the research you wish to conduct and whether you can combine any of the documents; if so, consider the requirements applicable to each document and ensure that your combined documents meets all 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.

Ensure that your proposed research protocol complies with applicable legal and ethical requirements.
Data Characteristic 8: Security

Security

Security refers to the means by which data is protected from unauthorized use or access.
Key Question: What is the form or medium of the data?

What It Means: Data exists in either tangible or intangible form. Intangible data is a fact that exists in a person’s mind or cellular or genetic information in a person’s body (e.g., DNA or blood type). Tangible data has been collected and/or extracted from an individual and exists in some form separate from the individual subject of the information. The medium of tangible data describes the means by which information is communicated, including on paper, digitally/electronically, as a preserved physical sample, or through in-person communication. Data can exist in both tangible and intangible forms as well as on multiple types of media simultaneously.

Why It Matters: Intangible data is generally not subject to health information security requirements. Tangible data may be subject to requirements that differ depending on the medium on which the data is stored. For example, the HIPAA Security Rule only applies to electronically maintained protected health information (PHI). Laws and regulations that establish security requirements based on form and medium include: HIPAA, Part 2, GINA, Privacy Act, state law.

Considerations for Next Steps: Consider the current form and medium of the data you wish to use and whether there are any legal requirements associated with that particular form and medium.

Key Question: Where is the data held?

What It Means: The medium on which tangible health information is stored must be in the physical possession of at least one entity; this can include the information collector, a recipient of the information, or the individual subject.

Why It Matters: Data may be subject to certain security requirements depending on where it is physically stored; the protections apply to the specific storage location and do not necessarily follow the data if it is moved to another physical location. Laws and regulations that govern physical security include: HIPAA, Part 2, GINA.

Considerations for Next Steps: Consider where the data you wish to use is stored, whether any security requirements apply to that particular location, and whether the data may be moved to a location with different or no security requirements.

Key Question: Who can access the data?

What It Means: Data can only be accessed by those with knowledge of its location and permission or authorization to physically access it.

Why It Matters: Security requirements may apply to data depending on who has been or may be permitted to access data. Laws and regulations that establish access limitations include: HIPAA, Part 2, Privacy Act.

Considerations for Next Steps: Consider whether the data you wish to use is subject to access restrictions and whether you must implement security requirement to limit access.

Key Question: What technical, physical, and administrative safeguards are employed to secure the data?

What It Means: Technical safeguards include items such as encryption, passwords, and antivirus software. Physical safeguards limit access to facilities, workstations, and devices that house data or may be used to access data (e.g., proper disposal of electronic media containing protected health information). Administrative safeguards include plans and policies for identifying security risks, preventing security breaches, monitoring security, and remedying security breaches and training employees on proper security procedures.

Why It Matters: Certain data may be subject to technical, physical, and/or administrative safeguard requirements. Generally, these requirements are flexible and may be tailored to the entity that maintains the data. Laws and regulations that establish these safeguards include: HIPAA, Part 2.

Considerations for Next Steps: Consider whether the data you wish to access is subject to administrative, physical, and/or technical safeguards and whether these are appropriately tailored.

Ensure that your proposed research protocol complies with applicable legal and ethical requirements.
Key Question
What are the researcher’s data management obligations once the data has been obtained?

What It Means
Identifiable information may be subject to a variety of security-related requirements, depending on the source, content, and/or intended use/purpose of the data. These requirements may be applicable to any recipient of the information, including a researcher, even if that researcher was not involved with the initial data collection.

Why It Matters
Researchers may have obligations related to data security for certain information, whether obtained from the subject of the information directly or via third party (such as a Covered Entity). These obligations may include requirements for technical and other security protocols (e.g., transmitting data using encryption), breach notification and reporting, and protection against re-identification of de-identified data.

Considerations for Next Steps*
Consider whether there are any security-related requirements applicable to the data you have obtained with which you must comply and whether you have the appropriate procedures in place to satisfy these requirements.

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 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

**Key Question**

Who owns the data?

**What It Means**

Data ownership generally refers to the lawful physical possession of data and/or the legal ability to restrict or control the data. Regardless of ownership, individual subjects of data may maintain certain rights related to the privacy and security of their data. Multiple parties may have ownership rights to the same information.

**Why It Matters**

Data ownership gives the owner the right to grant, restrict, or deny access to information. Where a Covered Entity is the owner of information, HIPAA also governs disclosure of the data (and other requirements relating to its use) may be determined by a contract, state law, or property law (including intellectual property law). Ownership of individual identifiable information, especially genetic information such as 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.

**Considerations for Next Steps**

Consider what entities may be able to claim an ownership interest in the data of interest. Then consider whether the owner is a Covered Entity or whether a non-Covered Entity can claim an ownership stake and from which the information may be more easily obtained.

**Are there contracts in place that govern how the parties to the contract or their agents may use the data?**

Examples of contracts that may govern data access, use, and exchange include a funding agreement between a grant funder and a grant recipient, a terms of service agreement between a database vendor and a researcher 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.

Access to data (and other requirements relating to its use) may be determined by a contract between the data seeker and data owner or holder. State law (including common law) governs construction and enforcement of contracts.

Consider what obligations may be required by any contracts in place, including how data must be handled and how it may be shared.

**What is the position/affiliation of the person seeking access to the data? Is there a legal relationship between the parties (e.g., employment)?**

Under the legal principle of agency, a principal party grants authority for another party, the agent, to act on the principal’s behalf in dealings with third parties. Employees are generally agents of their employers. Where the researcher is an agent of another party, such as a healthcare provider, the researcher has the rights and obligations of the healthcare provider.

Legal relationships may give a researcher a right to access data, such as when the researcher’s employer has purchased access to data or where the researcher’s organization is part of a corporate entity with the institution that holds the data. State law (including common law) governs legal relationships that create agency.

Consider the position of the parties seeking and holding data and whether existing relationships affect rights with respect to data access.

**Does any state law grant ownership rights or rights to restrict access?**

Some state laws, such as consumer protection and patient privacy laws, may confer rights and responsibilities with respect to access to data or data held by researchers.

Some state laws may confer rights that apply regardless of agreements between parties. For example, New Hampshire grants patients’ ownership rights over their health information. A patient may exert this right to prevent 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.

Consider what state laws may apply to the data you are seeking to 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.*