The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

APPENDIX B: ASSESSING POTENTIAL BARRIERS AND AMBIGUITY IN THE LEGAL LANDSCAPE

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

INTRODUCTION

Stakeholder discussions organized during the early part of the development of the Architecture (described in further detail in Chapter 1) raised a number of issues and concerns related to the use of various types of data for PCOR (discussed in Chapter 2) and navigation of the statutes and regulations that govern the use of this data for PCOR (discussed in Chapters 3 and 4 and Appendix A). The stakeholders further identified topics of particular concern ranging from consent to special populations to merging clinical and claims data.

This Appendix identifies and defines categories of issues (referred to as *gaps*) related to privacy and security requirements for PCOR and catalogues challenges and concerns raised by stakeholders according to those categories. Identifying the "gaps" in privacy and security laws and regulations relevant to PCOR depends on how "gap" is defined. The term is generally understood to mean either a space between two objects or a difference in points of view and is not often used in relation to the issues that arise with the privacy and security laws that govern PCOR; rather stakeholders and experts in the field typically use "challenges," "issues," or "barriers" when referring to concerns with these laws. The categories below were developed to catalogue the core issues that stakeholders and the relevant literature raise with respect to PCOR. These categories are meant to clarify the scope and depth of the issues raised, as well as to serve as a foundation for application of the laws and regulations to these issues. The issues may not technically be a "gap" in the traditional sense, but they are areas of concern to stakeholders that may indicate a need for additional policies or clarification of existing policies.

A. Statutory, Regulatory, and Policy Void
B. Ambiguous or Overlapping Federal Authority
C. Informal Guidance ("Soft Law")
D. Ineffective Regulation and Regulatory Bottleneck
E. Incompatible Stakeholder Implementation or Institutional Policies
F. State Law Variation
G. Ethical Issues
H. Legal/Compliance/Operational Issues
I. Additional Areas of Stakeholder Concern and Suggestions

The stakeholder comments and queries are expanded upon where relevant with commentary, analysis, and additional content, with the exception of stakeholder comments that related to operational or individual issues (e.g., institutional policy, technical issues, or preferred practices). Comments that addressed such organizational or individual issues, as opposed to issues with the content and scope of laws and regulations themselves, are catalogued separately under the Legal/Compliance/Operational Issues category and "Additional Areas of Stakeholder Concern and Suggestions" section.

A. Statutory, Regulatory, or Policy Void

Laws and policies are generally drafted to reflect past, current, and anticipated circumstances. A statutory, regulatory, or policy void arises when unanticipated events occur that either render existing laws or regulations obsolete or insufficient. Technological innovations often lead to (or are themselves) unanticipated events that make all or part of existing laws and policies incomplete. Recent examples of such innovations include the advent of mobile health technology and genetic testing. The use of virtual reality, 3D printing, synthetic biology, and nanotechnology in health care may lead to voids in the near future. Historical or structural changes also may render all or part of existing laws, regulations, and/or

policies irrelevant. This may occur if a new administration implements new policies that undermine the efficacy of existing laws or policies, if Congress passes a law that makes existing regulations moot, or if the Supreme Court declares a law unconstitutional, rendering all enacting regulations void.

A valid law or regulation may exist that addresses a specific topic, product, issue, or concept but may not do so thoroughly enough to address the needs of the field. This is another example of a statutory, regulatory, and/or policy void. A law or regulation may initially be drafted in a way that does not completely address a particular topic, creating a gap from the outset.

Examples/Analysis

- The secondary use of data is critical to certain types of research (especially as it relates to big data analytics and CER). However, the existing legal framework does not consistently nor completely address secondary use and/or re-disclosure of information. Part 2 discusses information re-disclosure by recipients, and the Common Rule 2017 Final Rule finalized provisions applicable to secondary use of identifiable biospecimens and identifiable private information for research (though these provisions do not go into effect until 2018). However, other laws (HIPAA in particular, with respect to re-disclosure by non-Regulated Entity recipients) remain silent on this issue.
- How should researchers manage re-consent when a participant's proxy changes during a longitudinal study?
- The availability of personal data, the creation of big data sets, and advancements in machine learning have led to concerns that the Privacy Rule's methods of de-identifying data, particularly the Safe Harbor method, are no longer sufficient.

B. Ambiguous or Overlapping Federal Authority

When Congress issues legislation (i.e., federal statutes), it generally authorizes and/or requires relevant federal departments (or agencies) to develop detailed regulations implementing the statute's various provisions. Many statutes grant federal departments broad discretionary authority to craft these regulations; typically, the relevant department Secretary delegates specific rule-making tasks to various departmental agencies. Multiple departments and agencies have oversight and rulemaking authority over the functional elements that relate to PCOR (e.g., the FDA regulates medical devices that capture data used in PCOR, SAMHSA regulates any use and disclosure of substance abuse treatment information). When multiple departments and/or agencies assert (or *can* assert) authority over parts of the same processes, stakeholders, or outcomes, each agency or department must clearly establish how it intends to exercise that authority. A gap exists when these boundaries have not yet been clarified, creating ambiguous or overlapping regulatory authority. The same issues are mirrored at the state level.

Examples/Analysis

- Federal authority that is ambiguous or overlapping is particularly apparent in the regulation of patient-generated health data (PGHD) and patient reported outcomes (PRO) data. The Federal Trade Commission (FTC; an independent federal agency) and the Food & Drug Administration (FDA; an agency within HHS) can each assert administrative and/or enforcement authority over some of the technology used to collect or transmit PGHD and PRO data (the FDA over mHealth devices that meet the definition of "medical devices" and the FTC over all mHealth devices). Simultaneously, both the FTC and the Office for Civil Rights (OCR; an HHS sub-agency) can assert administrative and/or

enforcement authority over the collection, use, and disclosure of PGHD and PRO data.[566] Specifically, OCR has authority over the use and disclosure of PGHD and PRO data by a HIPAA Regulated Entity, where the data meets the definition of PHI. The FTC has authority to regulate against unfair and deceptive trade practices pursuant to the FTC Act[567] and may bring enforcement actions against any parties that use unfair or deceptive methods to collect, use, disclose, or secure PGHD/PRO data (e.g., failing to disclose the scope of information collected, failing to use the security standards identified in the entity's privacy policy). The FTC also has authority to enforce the breach notification rule as it pertains to certain non-HIPAA regulated entities.[568] The end result of this regulatory scheme is that the mobile collection of sensitive health data and transmission to or from a provider could be subject to regulation by: (1) the FDA, in relation to the actual device; (2) OCR, in regards to the privacy and security of the data received by a provider; and (3) the FTC, in regards to the trade practices related to the device's manufacture or sale. The FTC's mobile health interactive tool helps illustrate the overlapping nature of these agencies' authority.[569]

C. Informal Guidance ("Soft Law")

Federal and state regulatory agencies often issue informal guidance regarding the agency's interpretation of its own regulations. Agencies may issue such guidance in a standalone document or include guidance in the preamble of a Notice of Proposed Rulemaking (NPRM) or a Final or Interim Final Rule. These guidance documents generally outline what actions the agency considers to be compliant with and/or in violation of its regulations. Informal guidance documents are legally nonbinding; conforming actions to the guidance document does not make a stakeholder immune from legal liability or an agency enforcement action (where such authority exists). While guidance documents officially issued by regulatory agencies can be used in court or administrative actions to defend against an enforcement activity, they are not dispositive. This introduces ambiguity because stakeholders cannot rely on nonbinding sub-regulatory guidance in the same manner or to the same degree as with a law, regulation, or contract.

---

[566] The Federal Trade Commission (FTC) regulates personal information pursuant to their authority over unfair and deceptive trade practices.

[567] 15 U.S.C. § 45; FTC, "FTC Policy Statement on Unfairness" (1980). *Available at*: https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (unfair acts or practices are those that cause or are likely to cause a substantial injury to consumers, cannot be reasonably avoided by consumers, and do not provide consumer or competitive benefits that outweigh the harms caused); FTC, "FTC Policy Statement on Deception" (1983). *Available at*: https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (deceptive acts or practices are those that include a material "representation, omission or practice that is likely to mislead the consumer).

[568] Health Information Technology for Economic and Clinical Health (HITECH) Act (Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115) at § 13407; 16 C.F.R. Part 318. (Note: authority is limited to Personal Health Record (PHR) vendors, PHR-related entities, and third-party service providers to either PHR vendors or related entities).

[569] FTC, "Mobile Health Apps Interactive Tool" (2016). *Available at*: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

Examples/Analysis

- The HHS Office of the Secretary, OCR, and the Centers for Medicare & Medicaid Services[570] (CMS; an agency within HHS) have released multiple pieces of guidance regarding compliance with various provisions of the HIPAA Privacy and Security Rules. Topics addressed include an individual's right to access their own information, methods for de-identifying information, HIPAA compliance for app developers, and disclosing information to family members.[571]
- The FTC, OCR, and FDA have each issued guidance regarding mobile health devices and information collected from these devices (i.e., PGHD/PRO data).
- While not "guidance" in the traditional sense, certain department or agency actions may be considered "soft law." For example, the CMS policy to redact all substance abuse patient information from its identifiable data sets is based on its interpretation of the 42 CFR Part 2 regulations. However, changes to the regulations made in the 2017 Final Rule relaxed limitations on research disclosures of information obtained from Part 2 programs. This change allowed CMS to include substance use disorder claims in the research identifiable files. As of 5/23/17, all research identifiable files include these claims. Further, researchers holding files impacted by the prior redaction are permitted to obtai "gap" files containing the redacte claims.

D. Regulatory Bottleneck

Regulations relevant to PCOR are often promulgated using a formal rulemaking process. An agency will publish an NPRM in the Federal Register, often accompanied by a request for [public] comment on some or all proposed provisions. After a specified time period, the agency reviews all comments received; if the agency chooses to take further action, it will modify, eliminate, or add to its proposed provisions based on this feedback. The agency publishes these modified provisions as a Final Rule in the Federal Register or, if the modifications warrant further public input, as a new NPRM or an Interim Final Rule (which contain binding regulations that may be changed or made permanent in a later Final Rule). Agencies may also issue an Advanced Notice of Proposed Rulemaking (ANPRM) or a Request For Information (RFI) as a means of soliciting feedback and information before proposing rules. The rulemaking process can take a long time to produce a Final Rule (if it produces one at all); this is particularly the case when the rules involve a complex and sensitive topic that requires careful deliberation. A Regulatory Bottleneck arises as a consequence of this process; a rulemaking signals that the regulatory structure applicable to a particular issue will [likely] change, so stakeholders do not know

[570] Note: CMS had administrative and enforcement authority over the HIPAA Security Rule until the HHS Secretary delegated such authority to OCR on July 27, 2009. Consequently, CMS is the author of Security Rule guidance issued prior to this date (*See* U.S. Department of Health and Human Services Office for Civil Rights (OCR). Delegation of Authority, 74 Fed. Reg. 38630 (Aug. 4, 2009)).

[571] *See* OCR, "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524" (*content updated* February 25, 2016). *Available at*: http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html; OCR, "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule" (*content updated* November 6, 2015). *Available at*: http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html; OCR, "Health app developers, what are your questions about HIPAA?" *Available at*: http://hipaaqsportal.hhs.gov/ (*last visited* September 25, 2017); OCR, Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care (n.d.). *Available at*: http://www.hhs.gov/sites/default/files/provider_ffg.pdf.

what the final provisions will be or when/if they will be finalized and the time between rulemaking and Final Rule keeps stakeholders in a holding pattern.

Examples/Analysis

- The changes to both the Part 2[572] and Common Rule regulations[573] significantly altered existing requirements regarding the use and disclosure of substance use information and federally supported research (in particular, mandating the use of a single IRB for multisite research, permitting broad consent for the secondary use of identifiable biospecimens and identifiable private information, and requiring changes to the informed consent process). However, regulators indicated at the time both Final Rules were published that further changes to each rule may be forthcoming. A Supplementary NPRM was published simultaneously with the Part 2 Final Rule seeking comment on numerous issues that make Part 2 incompatible with HIPAA (e.g., treatment and health care operations disclosures). No specific plans for further rulemaking were or have been announced since the SNPRM comment period closed in February 2017. In the preamble to the Common Rule 2017 Final Rule, the Secretary of HHS indicated that further changes to the Common Rule provisions are being contemplated and that harmonizing changes to Subparts B-E are anticipated. No formal rulemaking process was announced. Finally, the Common Rule 2017 Final Rule has an effective date one year after the Final Rule was published. It is possible that the effective date will be further delayed or that revisions to the updated regulations may occur prior to the effective date. Such uncertainty has led stakeholders to abstain from or delay conducting research rather than pursuing projects that could get undermined once the rules are finalized.

E. Incompatible Stakeholder Implementation or Institutional Policies

Laws and regulations often grant stakeholders discretion in deciding how to implement requirements. For example, the HIPAA Security Rule sets forth general standards for safeguards and allows Covered Entities to tailor their implementation to the Covered Entity's specific circumstances. Other laws and regulations may even allow stakeholders to decide which provisions, if any, to adopt. For example, the HIPAA Privacy Rule's permissive exceptions allow Covered Entities to select some, all, or none of the types/purposes of disclosures the rule allows. Gaps arise when stakeholders that must (or choose to) interact with each other have implemented flexible legal and regulatory requirements in ways that conflict, ultimately impeding their ability to conduct joint studies or share data. In addition, the law may be general enough to encompass many new fact patterns, but some stakeholders may be more risk-averse than others with respect to undertaking new activities or methods absent explicit approval by the relevant regulator. For example, advances in technology have outpaced regulatory action, leaving stakeholders to apply laws to new technology not in existence nor contemplated when the statute or regulation was initially drafted. In such a situation, stakeholders may choose not to engage with new technology at all or may limit their use of it to a narrow interpretation of the existing law.

[572] U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration (SAMHSA) Final Rule: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Final Rule") 82 Fed. Reg. 5485 (January 18, 2017).

[573] "Common Rule" Departments and Agencies, Final Rule: Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149 (2017).

Examples/Analysis

- Research institutions may implement the discretionary provisions of HIPAA, the Common Rule, and other federal and state laws and regulations in their own way, depending on institutional culture, business needs, and available resources. Institutional policies and procedures reflect these unique perspectives and thus may govern the same activity in an entirely different way than another institution. For example, an institution that focuses on biospecimens research will likely have processes and procedures that differ from an institution that primarily conducts research using data in electronic form. Inconsistency in policies and practices across institutions can make multisite research challenging. Common areas of a inconsistency include: (1) institutions requiring their own IRB or Privacy Board to approve a multisite study even though the study has already received approval from another IRB or Privacy Board; (2) differing procedures for data management, transfer, and record linkage; (3) differing requirements for both the content of and process for executing Data Use Agreements (DUAs); (4) differing policies related to use of minors' information; or even (5) an unwillingness to share data with an institution perceived as a competitor.
- Inconsistent implementation is also an issue with respect to health data registry structures, as the lack of consistent technical standards may limit a given registry's ability to be used for certain purposes (or for multiple purposes) and/or housing data from multiple organizations/organization types.

F. State Law Variation

There is significant variation in state laws governing health information, health information technology, medical practice, and public health data collection. State law variation can create gaps when research is conducted across multiple states or data is exchanged across state lines.[574]

Examples/Analysis

- States laws create and govern many of the public health registries that contain data relevant to PCOR.[575] Because these laws vary by state, the registries vary in terms of the scope of data collected, the variables captured, and the ability to disclose the data for research purposes.
- State laws vary regarding the collection or sharing of minors' information.[576] These laws may prohibit the collection of a child's information or require a parent to opt in to the collection of their child's information. Opt-ins have the potential to significantly reduce the amount of data available for research.
- States allow minors varying degrees of control over certain health care decisions and thus also over the information associated with those decisions (e.g., in some states, minors may unilaterally consent to treatment for sexually transmitted diseases, reproductive health, mental health

[574] 45 C.F.R. § 164.304 (2017).

[575] *See e.g.,* N.Y. Public Health § 2168 (Authorizing disclosure of identifiable information from the statewide immunization registry for research purposes); O.C.G.A. § 31-12-3.1 (Clarifying that the department may release vaccine registry data for scientific, educational, or public health purposes so long as the data are aggregated and do not contain names).

[576] *See e.g.,* MN 144.125 (Allows parents or legal guardians to consent to the use of their infant's blood sample and/or test results for research purposes); WAC § 246-650-050 (Requires the department to maintain newborn screening information and specimens until the child turns 21, but allows parents or guardians to request the destruction screening information/specimens once the screening process is complete).

treatment, etc.).[577] These laws impact IRB policies for obtaining consent for a minor's participation in research, for seeking consent once the minor reaches a certain age (i.e., re-consent), and their procedures for protecting and preserving or destroying data. The disparate nature of these laws and IRB policies may create issues for studies conducted in multiple states.

- State laws and regulations vary in regards to the rights of persons under the supervision of the correctional system.[578] These rights may change based on the person's status as incarcerated, paroled, or on probation, so researchers must account for how a participant's changed status will impact their project.
- State laws vary in regards to the definition and authority of legally authorized representatives (LARs; persons authorized by law to consent to another person's participation in research). State laws may prohibit LARs from receiving compensation in return for providing consent or may limit compensation to the expenses associated with participating in the study.[579]

G. Legal/Compliance Questions

Some of the issues raised by stakeholders are better conceptualized as questions regarding whether and/or how a law applies to a particular scenario. These questions may appear to be "gaps" because: (1) stakeholders have not [yet] obtained an answer from an attorney or compliance officer and assume the question is unsettled law, even though it may not actually be unsettled; (2) stakeholders have obtained a legal or compliance opinion that inaccurately represents and/or applies the privacy and security laws and regulations; (3) applying complex laws and regulations to a particular situation can be extremely challenging (particularly for stakeholders without a legal background); or (3) institutional policies and procedures that include heightened protections reflecting the institution's culture, resources, and/or tolerance for risk are perceived as the floor for legal protections, even if those procedures are more stringent that what is legally required at the floor level. The questions below are answerable within the existing legal framework for privacy and security (i.e., do not represent gaps in those protections), and most are highly fact-specific (i.e., the answer will depend on the details of the exact scenario in question, including the state(s) in which the activity occurs, the relevant institution's policies and procedures, the characteristics of the individuals involved in the research, etc.). Stakeholder questions that fall under this category included the following:

Examples/Analysis

- How do the Part 2 regulations and state substance use privacy laws affect the secondary analysis of identifiable data?

---

[577] *See e.g.,* Arkansas Code Ann § 20-16-508 (Allowing minors to consent to STD treatment, but granting providers discretion to inform the minor's parents or guardian of the treatment); Idaho § 39-3801 (Allowing minors aged 14 or older to consent to the treatment of infection, contagious, or communicable diseases).

[578] *See e.g.,* CA Penal Code § 3501 et seq. (Prohibiting biomedical research on prisoners in California, but providing a limited exception for investigational drugs); A.R.S. § 31-321 (Allowing prisoners to consent to participate in research programs that receive approval from the director of the department of corrections).

[579] *See* CA Health & Safety Code 24178 (Identifying the persons that may provide surrogate consent to research participation and prohibiting surrogates from receiving compensation in exchange for consent).

- Birth and death information are vital statistics that are required to be reported to states. Misuse of this information—e.g., identify theft—can cause significant harm. Given this concern, what are the legal implications of linking research data with vital statistics?
- Are researchers and third party entities legally required to use an internal IRB when linking data?
- How does a prisoner's incarceration status impact the consent process? For example, when a research participant is incarcerated, do they need to re-issue consent before a researcher uses data collected prior to their incarceration?
- What are the rights and responsibilities of Legally Authorized Representatives (LAR)? What legal obligations does a researcher have when a patient and their LAR disagree about a course of action (e.g., an LAR consents to a patient's participation in a study, but the patient asks for his or her data to be removed)?
- What are a researcher's legal obligations in regards to the disclosure of genetic information that affects the family members of a research participant? Can a researcher be held liable for disclosing or failing to disclose this information to affected family members?
- Do state laws impact the collection of data from workplace wellness programs?
- Do researchers have a legal obligation to disclose life-threatening diagnoses? Can they be held liable for disclosing or failing to disclose this information?
- How and when should a researcher contact participants about study results? Should informed-consent procedures address the method and timing of such disclosure?
- Many sensors allow individuals to transmit their information to their provider's EHR. Since the sensor data are combined with the individuals' other data (input by the provider in the EHR), researchers who have obtained consent to access EHR data can generally access the sensor data as well. How should researchers obtain consent if the sensor data flows to researchers through a non-EHR pathway?
- Are there legal implications to releasing research results through a patient portal?
- Do research protocols need to include a method for determining perspective participants' capacity to consent?
- Given the privacy concerns inherent in conducting research on American Indian/Alaskan Native (AI/AN) populations, are there best practices that can guide researchers' collection of identifiable information when these populations participate in a study?
- Does PRO data fall within the category of clinical data that providers must report to PH registries?

H. Ethical Questions and Concerns

PCOR potentially implicates many ethical concerns, as researchers and policymakers must balance patient privacy interests and the possibility that research might adversely impact or disproportionately advantage certain populations against potential research benefits. Ethical questions and concerns by stakeholders include the following:

Examples/Analysis

- If access to substance use data without direct patient consent is legally permissible, is such access by researchers ethical?
- Should researchers inform individuals of the privacy implications that arise when their birth certificate is used for research purposes?
- Is it ethical to use perpetual consent in the PCOR context?

- What are the ethical implications of using an opt-out consent for participation in PCOR as opposed to opt-in consent?
- Stakeholders believe that participants must retain autonomy over their data and that policies and procedures must exist to safeguard this autonomy. The importance of autonomy exists even if a participant's cognitive capacity is in decline.
- Stakeholders believe that research on prisoner populations must include additional measures to ensure proper consent for data release and safeguards against coercion. Stakeholders noted that data from incarcerated individuals raises unique privacy concerns (e.g., court-compelled data disclosures could affect the individual's release, parole, or probation).
- The collection of genetic information during a study may reveal that the participant has a genetic condition, is at risk of developing a genetic condition, and/or their family members are at risk of developing a genetic condition. Ethical concerns thus arise regarding the disclosure of such information by researchers to participants and/or their family members and disclosure by participants to their family members.
- Genetic research also raises issues in that the results could be used to discriminate against people with certain genetic characteristics.
- Research that involves small, culturally unique populations raises ethical issues. Notably, the risks to participant privacy might be greater because the small, unique nature of the population may make de-identified data easier to re-identify. The burdens associated with ensuring adequate protection of small, culturally unique populations might result in researchers choosing not to pursue research projects with these populations. This choice could be viewed as favoring population autonomy and privacy, but it also deprives populations of potentially beneficial insights that could help their communities. The stakeholders noted that researchers working with AI/AN populations must be aware of the sensitive nature of such research, given the historical oppression of these populations and abuses that have occurred within the research context.

I. Additional Areas of Stakeholder Concern and Suggestions

Finally, some of the stakeholder comments question the feasibility of certain compliance methods and/or suggest methods for complying. These suggestions are not "gaps" in law or policy and therefore will not be reflected in future deliverables for this project, such as the data flow mapping or framework. However, agencies may wish to consider these suggestions when developing guidance for stakeholders.

Examples/Analysis

- Stakeholders identified a decision tree as a potential tool to help researchers determine when and how to disclose study results to participants.
- Institutional policies and practices regarding data linking and IRB/Privacy Board review make multisite research studies difficult to conduct. Stakeholders suggested using a Memorandum of Understanding (MOU) as a method of reducing these challenges.
- The form and procedures associated with consent depend on the purpose of the consent (e.g., consent to use of data for PCOR versus consent to participate in clinical trial). Stakeholders suggested developing standards for IRBs regarding such context-based consent forms.
- Stakeholders suggested that a compound consent and authorization form could be used to facilitate the linking of data held by one research entity to data held by another entity.
- Is it feasible for a qualified independent entity to assess a potential research participant's capacity?
- Is there a feasible method for tracking prospective participants' capacity consent? Does this method work in longitudinal studies?