I. Introduction

Statement on Protecting Patient Privacy

February 26, 2024

PCORnet, the National Patient-Centered Clinical Research Network ("PCORnet"), an initiative of the Patient-Centered Outcomes Research Institute ("**PCORI**"), comprises a community of patients and their families, researchers, scientists, clinicians, health systems, and other committed individuals and organizations dedicated to the common purpose of accelerating patient- centered outcomes research. Through this partnership, and within an environment of mutual trust and shared responsibility, PCORnet is transforming the culture of clinical research from one directed by researchers to one driven by the needs of patients and those who care for them.

This Statement on Protecting Patient Privacy describes the practices in place to protect the privacy of individuals ("**Patients**") whose healthcare-related data are made available to researchers through the PCORnet infrastructure. This Statement is endorsed by the work of the Clinical Research Networks and their individual contributing Network Partners ("**CRNs**"), the PCORnet Coordinating Center, and the researchers who use the data and services made available through PCORnet.

Data utilized by CRNs originate in the health care system, from health care providers and/or payer organizations; therefore, these networks refer to the data they hold as "patient data."

The CRNs and the Coordinating Center comply with the Data Sharing Agreements executed between the CRNs and the Coordinating Center. Data Sharing Agreements may include both the PCORnet Master Data Sharing Agreement that addresses sharing of data for administrative and analytics queries, as well as additional Data Sharing Agreements that are executed in the context of funded research projects. (See Use of Patient Information in PCORnet.)

II. The PCORnet Privacy-Protective Infrastructure

As a patient-centered initiative, patient engagement and the protection of individual privacy are core values for PCORnet. Patient privacy is deeply rooted in the PCORnet infrastructure, data flows, and technology architecture. CRNs within PCORnet have standardized their existing electronic health record data against the PCORnet data model (called the Common Data Model, or "**CDM**"). These data remain behind institutional firewalls. Some CRNs operate in a centralized fashion, where data from several Network Partners are managed by a single entity. Other CRNs operate in a more decentralized fashion, where the CRN Network Partner (not the CRN itself) maintains the CDM locally; for ease of understanding, when referring to "CRNs", we

mean the actions of a centralized CRN acting on behalf of its Network Partners or those of an individual Network Partner operating in a decentralized CRN (unless otherwise noted).

In order to access these data, queries are centrally programmed and distributed by the PCORnet Coordinating Center and executed locally by the CRNs. The CRNs then securely return the minimum amount of data necessary for the request to the Coordinating Center for compilation and sharing.

The PCORnet Privacy-Protective Infrastructure illustrated in Figure 1 lies at the heart of PCORnet privacy protections. This section summarizes the framework and its privacy-protective features. Each of these features is further detailed in the sections that follow.

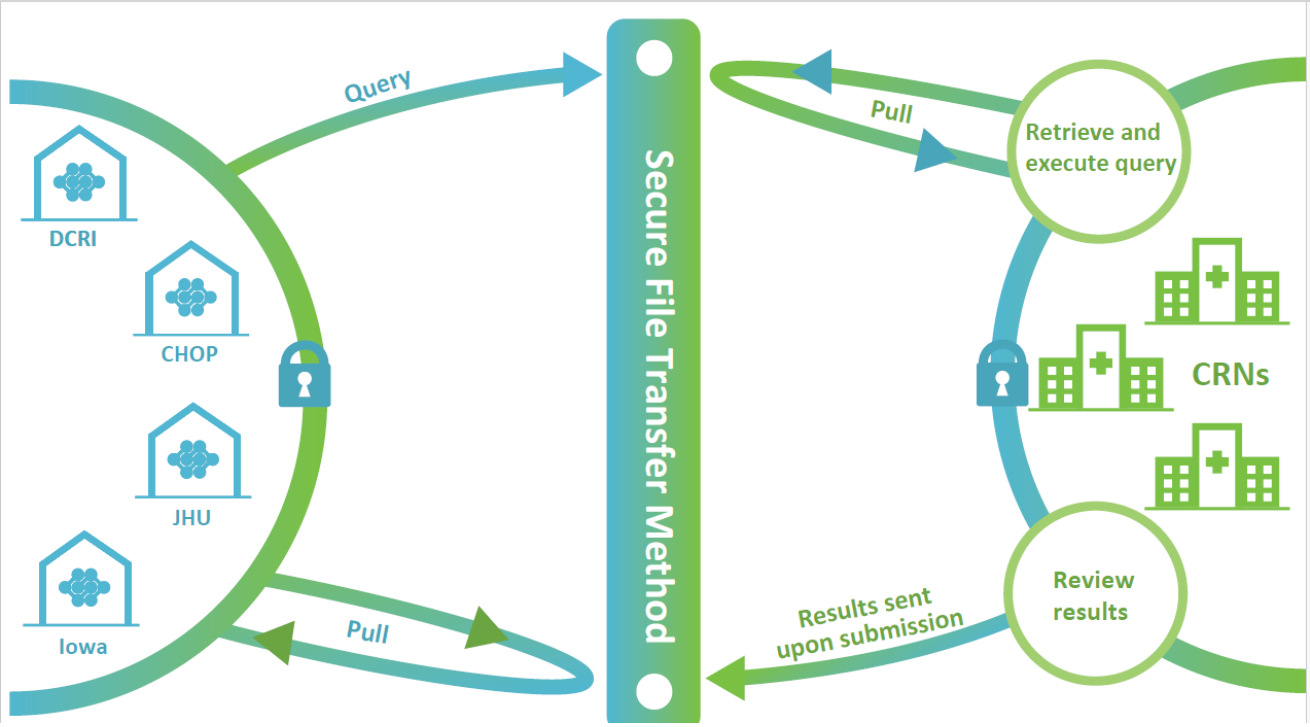

Figure 1. The PCORnet Privacy-Protective Infrastructure supports a broad spectrum of patient-centered research, while protecting individual privacy.

The PCORnet Privacy-Protective Infrastructure depicted in Figure 1 enables any researcher planning for or conducting a research project (a "**Requestor**") to submit a query request to the Coordinating Center. Some Requestors are researchers affiliated with PCORnet or one of the CRNs, while others may be external to the network.

The Coordinating Center reviews each query request, and if it abides by the current PCORnet Query Guidance, formats it in a manner consistent with all PCORnet queries and distributes it to Network Partners or CRNs through the PCORnet Secure File Transfer Method. The PCORnet Secure File Transfer Method serves as the primary data sharing hub between the Coordinating Center and the CRNs and is a key privacy-protective feature of the PCORnet infrastructure. The PCORnet Secure File Transfer Method is a secure cloud-based platform.

CRNs make the determination of whether to respond to the query request. If so, the CRNs send back query results to the Coordinating Center. (See PCORnet Query Methodology.)

III. Collection of Patient Information by the PCORnet CRNs

The PCORnet CRNs are largely affiliated with health care providers, who typically capture information in the form of data derived from electronic health records (EHRs), though some have relationships with health plans, who provide data derived from administrative claims.

These data are standardized into the Common Data Model (CDM), which CRNs use to respond to queries. Data within each CDM exist as a Limited Data Set, as defined by the HIPAA Privacy Rule. Limited Data Sets are comprised primarily of data in which all of the 18 HIPAA "identifiers" enumerated in the HIPAA Privacy Rule have been removed, other than dates of service, ages, and Patient location above specific street level (e.g., state or zip code).

In addition, the CRNs may collect data generated through research studies, but only if allowed by IRB-approved protocols, Data Sharing Agreements, and individual Patient consent, as applicable.

IV. Sharing of Patient Information with the PCORnet Coordinating Center

The CRNs share data with the PCORnet Coordinating Center primarily as aggregate data. The CRNs may also share individual-level data with the Coordinating Center, which generally is in de-identified form or is part of a Limited Data Set; identifiable data is shared only as permitted by applicable law, the Partner Network policies, IRB approvals, and individual Patient consent, as applicable.

V. Use of Patient Information in PCORnet

Data collected by the CRNs are used to support activities to prepare for research, such as queries to determine size or characteristic of a research cohort (a group of research subjects with a common characteristic). In addition, data collected by the CRNs are used to support research studies in compliance with law and relevant regulations. PCORnet CRNs may choose to participate in specific research protocols and protocol development at their own discretion.

PCORnet facilitates multi-center observational and interventional studies that may be funded by PCORI or by external public and private funding sources. PCORnet enables external researchers and funding organizations to contract for use of PCORnet services and infrastructure for individual studies, with separate and appropriate agreements in place to support those activities.

PCORnet and CRNs must comply with all federal, state, and local laws and regulations related to individual privacy, the security of health and personal data, and the protection of human subjects involved in research. Relevant federal law includes the Federal Policy for the Protection of Human Subjects (the Common Rule) (at 45 C.F.R. Part 45) and the Health Insurance Portability and Accountability Act and its implementing regulations at 45 C.F.R. Parts160-164 (collectively, "HIPAA").

To comply with the Common Rule, all PCORnet studies that meet the definition of human subjects research must be reviewed by an IRB and must be performed in accordance with the Common Rule to assure fairness, privacy, and ethical treatment of the individual Patients whose data are used in the research. An IRB may require a Patient to execute an informed consent form to participate in the research, or an IRB may waive informed consent if the regulatory requirements for waiver are met.

To comply with HIPAA, health care providers and health plans ("covered entities" under HIPAA) may provide protected health information ("PHI") for activities to prepare for research, such as determining whether a sufficient number of records exists to support a research protocol. To use Patient data for a research protocol, HIPAA provides multiple "paths" for compliance: (1) Patient authorization (which may be integrated into an informed consent form); (2) IRB waiver of Patient authorization (if the regulatory requirements for waiver are met); (3) use of a Limited Data Set under terms set forth in a Data Use Agreement; or (4) use of only de-identified information that meets the requirements of the HIPAA de-identification standards.

In addition, PCORnet conforms to the HIPAA "minimum necessary" rule by collecting only the information needed to fulfill a PCORnet study, by adopting a data model that excludes personal identifiers, by restricting query responses to aggregate data where possible, and by limiting the number of people authorized to access data.

VI. PCORnet Query Methodology

Requests for a PCORnet query are submitted to the PCORnet Coordinating Center. The Coordinating Center then reviews the request for compliance with current PCORnet Query Guidance, formats it as a PCORnet query, and distributes it to CRNs through the PCORnet Secure File Transfer Method. Each receiving Partner Network reviews the query and independently decides whether to execute it against the CDM data held in its network. Only authorized and authenticated users, as set forth by the Network Partner, may upload responses to queries for return to the Coordinating Center.

Every PCORnet Query must include detailed information about the research the query supports. This information includes several considerations to protect individual Patient privacy:

- A summary of the ways in which data returned may be altered, disclosed, re-identified, or otherwise used.

- Notification if the query requires person-level data.
- If the query requires the release of person-level data, a specification of the approach to be used to de-identify the data and a description of any anticipated risks for any population that could be impacted by the analysis.

The PCORnet standard method for minimizing the risk of identification from aggregate values is through the enforcement of minimum count thresholds – sometimes referred to a minimum "bin size" or "cell size"—by requiring that a minimum number of individuals be represented in any bar in a histogram ("bin") or any single "cell" in a spreadsheet. For example, if the query yields an aggregate response of "1 person found," then an adversary might be able to infer the identity of that individual based on the parameters entered with the query. To counter this risk, PCORnet has established a minimum cell-size threshold of 11 for all PCORnet data queries prior to disclosure to the requestor or public venues (as specified in the PCORnet Master Data Sharing Agreement).

VII. Data Linkage

PCORnet has implemented a mechanism for linking data across the CRNs in a manner that preserves privacy, called the privacy-preserving record linkage (PPRL) solution. Very few CRNs capture all health care for their Patient populations. One way to bridge this gap is to link records in a privacy-preserving manner across the CRNs that have overlapping Patients.

PCORnet has implemented a PPRL solution in which software is installed locally at each CRN Network Partner and encrypted "hash tokens" are generated based on personally identifiable information ("**PII**") held within their source systems. It is not possible reverse engineer the tokens in order to re-identify the patient. The software allows the Coordinating Center to compare tokens coming from multiple CRNs and determine that they correspond to the same Patient, but the Coordinating Center will not be able to tell who the Patient is. These tokens have been determined to be de-identified data under the HIPAA Expert Determination method.

VIII. Security of Patient Information

The security of the PCORnet infrastructure architecture is a significant means through which personal information is protected. To help assure that all Patient information is adequately protected from unauthorized disclosure, modification, and destruction, all PCORnet CRNs and the Coordinating Center are required to implement the administrative, physical, and technical safeguards described in the HIPAA Security Rule (at 45 C.F.R. Part 160, 164). The Security Rule requires continuous protection of protected health information against reasonably anticipated threats and hazards, conditions, uses, and disclosures.

IX. Patient Engagement and Transparency

As a patient-centered initiative, Patient engagement and transparency are core values for PCORnet. PCORnet is committed to assuring that Patients and the public are given open access to values and practices of PCORnet, so that Patients can understand how PCORnet protects data about them.

Patients also play prominent leadership roles in all of the CRNs. In each CRN, patients serve as representatives in local governance, representing Patient interests at the Network and PCORnet levels. Patient representatives also hold seats on the PCORnet Steering Committee and are actively engaged in developing and overseeing practices to protect patient privacy.