Colorado Health Observation Regional Data Service (CHORDS)
Governance Plan
Version 2.1

I. Introduction

The Colorado Health Observation Regional Data Service (CHORDS) began in 2011. It is a regional collaborative partnership among Colorado health providers, public health departments, the Colorado Regional Health Information Organization (CORHIO), and the University of Colorado Anschutz Medical Campus to share health data. CHORDS collects, analyzes and presents data from participating partners' electronic health records (EHRs) to monitor population health, target areas for intervention, and conduct research and evaluation activities.

CHORDS uses a distributed data approach in which data partners maintain physical and operational control over their electronic data stored in virtual data warehouses (VDWs). CHORDS will aggregate data across data partners, not revealing the source institution. Individual, record-level data may be provided with the appropriate approvals in place, including approval by participating data partners as well as relevant committees (Executive, Governance, Research Council, etc.).

CHORDS is committed to patient privacy and believes that the protection of privacy, confidentiality, and data security is essential to the existence and success of public health monitoring and research. All data are securely exchanged through a web-based, password protected portal accessible only by approved users. The CHORDS database (CHORDS VDW) meets the Health Insurance Portability and Accountability Act (HIPAA) definition of a limited data set. All CHORDS public health queries are executed to remove protected health information (PHI) before information is shared and adhere to privacy-preserving guidelines. Data partners and data users are responsible for proper stewardship of CHORDS data in their possession.

This document establishes governance policies and guidelines based on the guiding principles of good will, trust and appropriate stewardship of data among all participating Network partners. It addresses activities, duties and expectations regarding data curation, query processing, permitted data uses, participating partners' rights and responsibilities and other topics. This document identifies a governing structure to implement guidelines, oversee CHORDS' development, operationalize changes and engage stakeholders.

This governance plan will align policies, guidelines and processes for public health monitoring, evaluation and research activities to reduce costs of parallel structures and operations, reuse knowledge and support a learning health system.

These policies and guidelines are flexible. They will be revised as needed to meet changing circumstances and reviewed at least annually. When necessary for specific research activities, supplemental materials will be developed and stored with CHORDS documentation pertaining to the applicable research project. Only when a given artifact is useful for Network operations will it be included as an Appendix to the Governance Plan.

Revision History

Revision Number	Date	Comment
Version 1.0	11/16/2016	First draft to Governance Committee
Version 1.1	12/2/2016	Project development work group created, revised public

		health presentation and publication guidelines and appendix documents.
Version 1.2	12/19/2016	Revisions based on Governance Committee member comments.
Version 1.3	2/15/2017	Added CHORDS Network graphic; incorporated revisions from Governance Committee members; moved Revision History.
Version 1.4	08/17/2017	Added details on research governance throughout.
Version 2.0	2/28/2019	De-duplication/use of ID from CORHIO, Councils updated, committee and CHORDS VDW language clarified, additional research governance information.
Version 2.1	4/14/2020	Standardization of language regarding technical partners and network-wide identifiers, updated Appendices.

A. Guiding Principles

CHORDS is committed to public health surveillance and research that improves the health of Coloradans.

CHORDS is a collaborative project that relies on the good will and trust of participating Network partners. Essential to this trust is appropriate stewardship of private and confidential health information.
Each partner respects and honors the autonomy of their site and others and recognizes the benefits and responsibilities of using this information to serve public health and research.

The following principles reflect the core values that guide the governance process and are reflected in the governance plan.

I. The Governance Committee will:

- Establish, document and conduct transparent decision-making processes.
- Facilitate high-quality monitoring, evaluation, research and health improvement activities.
- Identify and address new governance issues as necessary.
- Review, revise and approve governance policies on an annual basis or more frequently as needed.

II. Data Partners will:

- Retain autonomy in sharing their data.
- Provide efficient stewardship of site and network data by leveraging resources.
- Engender collaboration and leadership within CHORDS.
- Strengthen and ensure compliance with site-specific, local, state and federal policies and regulations.

III. Technical Partners will:

- Comply with data sharing agreements they maintain with data partners
- Provide efficient stewardship of site and network data by leveraging limited and existing resources.
- Engender collaboration and leadership within CHORDS.
- Strengthen and ensure compliance with site-specific, local, state and federal policies and regulations.

IV. Data Users will:

- Adhere to responsibilities for data access and use.
- Use data to enhance evidence-based, integrated health care and public health practice.
- Foster innovative research and monitoring methods to address and improve health.
- Assess population measures and discover generalizable knowledge for the public domain.
- Encompass diverse perspectives: patient-centered, population-based, provider and health delivery systems.
- Maintain participating data partner confidentiality by never attributing data to a site nor comparing data from one partner site with data from another unless authorized by data partners to do so.
- Rapidly disseminate findings into the public domain.
- Be vigilant in protecting patient confidentiality and privacy.
- Engage stakeholders regarding data, findings and population metric decision-making.
- Provide aggregate data and public recognition to data partners when requested.

B. Scope

CHORDS was initially established by partner organizations affiliated with the Colorado Clinical and Translational Science Institute (CCTSI). It has grown and developed using funding from several federal, state and foundation public health surveillance and implementation grants and contracts.

In 2015, the Colorado Health Foundation awarded the Colorado Health Institute (CHI) a two-year, $1.9 million grant to support activities including updating CHORDS technology, expanding CHORDS data partners and users, developing a formal governance structure and establishing a sustainability plan so CHORDS can continue to develop in the future. The Colorado Health Foundation provided an additional two years of funding in 2018 to continue developing the CHORDS Network and support its transition to CORHIO. CHI serves as the convener for the CHORDS Network (see figure below).

CHORDS is currently supporting public health activities in the Front Range region of Colorado. Initial priority areas of focus for public health include cardiovascular disease, diabetes mellitus, mental health, obesity, and tobacco use. CHORDS began in the Metro Denver region and has expanded to include data partners and local public health agencies in northern Colorado.

CHORDS can also support research (e.g., observational, clinical, or health services studies) across multiple institutions.

CHORDS is committed to student education at numerous degree levels. The Network is exploring options for supporting appropriate student projects that balance available time and resources and meet the sustainability mission.

Specific aims for CHORDS include:

- Advance trustworthy, efficient, responsive and regulation-compliant data sharing in support of collaborative, regional public health initiatives and research, across patient populations.
- Expand network scale and utility toward an array of public health and research activities.
- Engage a broader community of stakeholders to maximize overall utility.
- Develop a community-engaged, sustainability plan.

CHORDS Network (see Appendix A**.)**

II. Organizational Structure

CHORDS governance consists of a Governance Committee and Executive Committee, Participants, an Advisory Council for Research, and Work Groups. Participation in these bodies is voluntary. These bodies and the organizational structure may evolve as the Network identifies a sustainable home for CHORDS.

CHORDS is not a legal entity; therefore, each organizational partner within the Network must first adhere to the policies and procedures of that organization as well as CHORDS data sharing agreements.

While the CHORDS infrastructure, including PopMedNet (PMN), is housed at CORHIO, the Network is governed by the guidelines and principles articulated in this document.

A. Governance Committee

The Governance Committee has overall responsibility for CHORDS, providing leadership and accountability in the following areas:

- Strategic direction;
- Financial coordination and sustainability, including guiding and overseeing grant applications and budgets, and identifying new resources;
- Initiatives and projects, including research;
- Recruiting new data partners; and
- Formalizing relationships among data partners, including executing data agreements.

The Governance Committee consists of data partners, data users and key stakeholders including community members and technology partners. All data partners and data users will be invited to designate one Governance Committee member. Members with multiple roles in CHORDS may represent only one role while serving on the Governance Committee.

The Governance Committee will have a chairperson and will designate five Members to serve on the CHORDS Executive Committee. Members may also serve as chairpersons for CHORDS Advisory Councils and Work Groups.

B. Executive Committee

The Executive Committee represents the CHORDS Network among external stakeholders and identifies growth opportunities for Governance Committee consideration. The Executive Committee is also charged with guiding and informing the Governance Committee's strategic direction and preparing items for its consideration and review. The

Governance Committee may charge the Executive Committee with decision-making authority in certain circumstances to allow the Network to be more nimble and efficient and reduce response time for time-sensitive issues.

The five-member Executive Committee provides balanced representation of CHORDS data partners, data users, and stakeholders.

The Executive Committee will make recommendations to the Governance Committee regarding activities and responsibilities tasked to the Advisory Council or Work Groups.

C. Participants

1. Data partners

Data partners are organizations that provide health observation data to be queried by CHORDS data users. Data partners include health care and mental health providers that establish connections between a virtual data warehouse and the CHORDS network using PMN to participate in CHORDS requests. CHORDS will continue to explore how data partners' data can be integrated with other data sources to support public health and research goals. A current list of data partners is available on the CHORDS website.

2. Technical Partners

Technical Partners are organizations that provide services to catalog, curate, manage or improve data from data partners. Technical Partners include the Colorado Department of Public Health and Environment (CDPHE), for geocoding of health observation data; the Colorado Community Managed Care Network, which serves as an intermediary managing data for Community Health Centers; the Adult and Child Consortium for Health Outcomes Research and Delivery Science (ACCORDS) which leads CHORDS development activities; and CORHIO which houses CHORDS' infrastructure and provides identity management services.

3. Data users

Data users request partner data for public health monitoring and evaluation, as well as for research studies. Data users must have legal agreements with data partners (Appendix B.) and complete the CHORDS User Access form (Appendix C). Current data users are described below.

a. Public health agencies

State and local public health agency officials use CHORDS to monitor population health, target and evaluate interventions and collaborate with communities to support health. Public health data users participate in a CHORDS Data Users Community of Practice, convened by the CHORDS Project Manager for Public Health (PMPH), to discuss public health uses for CHORDS data.

b. Researchers

Researchers, including students, from a variety of fields such as medicine, public health, behavioral health, pharmacy, sociology and anthropology may seek permission to use CHORDS data to answer clinical and health services research questions. The use of data for research purposes will require vetting of ideas, different legal, regulatory and institutional review agreements than data used for public health activities.

The Governance Committee may further expand the types of users in the future.

CHORDS engages community partners in several ways. Public health data users work with community organizations and residents within their respective jurisdictions to identify the most important questions to be addressing through CHORDS. Through the Data Users Community of Practice, public health users also identify priorities for future uses as well as recommend opportunities for further dissemination.

The Network also seeks direct feedback from community members about the products being developed using CHORDS data as well as priorities for future uses. Network participants, led by members of the Data User Community of Practice, will engage with at least one community group annually, or more frequently if needed, to solicit feedback on recent maps and adapters, processes for community members accessing CHORDS information, and discuss how CHORDS can inform community activities. These groups may include local health alliances and community advisory panels.

D. Advisory Council - Research

The Advisory Council – Research (Research Council) includes representatives from the University of Colorado Anschutz Medical Campus, funders, data partners and community-based research organizations. The Research Council reviews research project proposals to assess fit and feasibility and makes recommendations to the Governance Committee regarding project approval. The Research Council monitors all phases of ongoing research projects from grant applications to manuscript preparation. The Research Council is also a forum to discuss the direction of the CHORDS research agenda as well as CHORDS developments across the network and their potential impact on CHORDS' research activities. The Council meets as needed, but at least twice a year and is chaired by a Network member.

E. Work Groups

Three Work Groups made up of CHORDS data partners and data users address operational issues. The Governance Committee may decide to create additional Work Groups at any time as needed. Work Groups are convened and staffed by a Network member. Work Groups will meet at least quarterly.

1. Data Work Group
   The Data Work Group is responsible for identifying requirements and standards for data curation, exchange and use. The Data Work Group will also develop quality assurance (QA) activities for the Network. The Data Work Group oversees the process for defining the data model, proposing modifications including new tables and variables or changes to existing ones and scheduling their implementation. This group also plans query interface changes; and is responsible for activities related to data definition and harmonization, and data QA. These activities may require use of confidential data not for public release. The Data Work Group may convene a Community of Practice among data partners around specific data related needs.

2. Network Operations Work Group
   The Network Operations Work Group is responsible for day-to-day oversight of CHORDS operations, including installing, testing, maintaining and developing CHORDS data sharing software. The group advises the Governance Committee on the pros and cons of software upgrades when needed. This group is also responsible for implementing all network access and security privileges for data partners and data users, including scheduling of technical activities and identifying necessary resources; and prompt reporting of any data privacy or security incident to the Governance Committee, affected organizations, and appropriate regulatory authorities.

3. Project Development Work Group

The Project Development Work Group is responsible for fostering high-quality monitoring, evaluation, and quality improvement activities through CHORDS. This may include assisting users in crafting their questions, assessing project feasibility and advising the Governance or Executive Committees on prioritizing opportunities to demonstrate the value of the CHORDS Network. The Project Development Work Group develops and reviews new and existing projects and advises on public health uses; and manages a spectrum of project planning and timelines. It will work with existing data users and engage new ones. The Project Development Work Group may convene a Community of Practice among data users around specific projects and opportunities. As the need arises, separate subgroups may be convened for public health users and researchers.

Work Group and the Research Council charters are in Appendix D.

III. Decision-Making Strategies and Policies

A. CHORDS Network

Members of the Governance Committee are responsible for decisions that impact the CHORDS Network. Recommendations to the Governance Committee may come from the Research Council, Work Groups, and/or partners. The Governance Committee recognizes that each organizational partner is bound by the policies and procedures of that organization, as well as CHORDS data sharing agreements.

B. Decision-making Procedures

The CHORDS Governance and Executive Committees, Council and Work Groups will follow CHORDS decision-making procedures. Consensus-based decisions are preferred; however, decision-making processes will vary depending upon the issue. The chairperson of the Committee, Council or Work Group will decide, with input from the members, whether to seek consensus or use a voting process and how to carry out either process.

When a consensus-based approach does not result in a decision, or when voting is preferred, a simple voting process will be used so activities can move forward. Formal votes require a quorum (more than 50 percent of members). Members may abstain or recuse themselves from any vote. Each member is entitled to one vote; data partner and data user organizations are limited to one vote based on their designated role on the Committee, Council or Work Groups. A motion carries when a simple majority (51 percent of those present) is reached. Votes may be taken verbally or using web-based voting software. Individual votes may be public or anonymous. All decisions will be documented and include a rationale.

C. Conflict of Interest

The Network relies on its partners' active participation and input on decisions. Partners may have conflicts of interest for certain decisions regarding the CHORDS Network. These include a potential for deriving profit or financial gain.

In the spirit of disclosure and transparency, partners will share any potential conflict during the deliberation process and recuse themselves from voting on the matter. Disagreement over the presence or absence of a potential conflict among any partner will be brought to the Executive Committee for a decision.

D. Policy Enforcement

The Governance Committee is responsible for upholding CHORDS guiding principles and enforcing CHORDS policies and guidelines. The Governance Committee may delegate certain oversight activities to the Executive Committee.

Emphasis will be placed on prevention or early detection of noncompliance with Network policies, with prompt and confidential communication with data partners or data users who are not following policies or are at risk of compromising established policies.

E. Dispute Resolution
Efforts to resolve disputes between data partners, data users and other members of the CHORDS Network will begin at the most decentralized level. If resolution is not achieved, the Executive Committee will be alerted so it can advise and assist in the process. If the dispute still cannot be resolved, the Committee will make a final decision.

F. Stakeholder Role in Policy Development and Decision-making
Members of the Advisory Councils are important resources to consider issues or identify concerns. Members should be included in deliberations wherever possible, as their time and interest allow.

G. Projects or Requests for Collaboration
Suggestions for projects or requests for collaboration may arise from multiple sources inside and outside of the CHORDS Network. The Governance Committee is responsible for identifying, and securing when appropriate, funding and resources as needed to carry out projects.

1. Public Health
Public health data users may request data to support regional collaboration between authorized CHORDS data users and other public health agencies. One public health data user may initiate a request on behalf of other users. Public health agencies may also request data that will be used by community partners to inform shared activities. It is up to the public health agencies to decide if the data being shared and the community partner fit within the mission of CHORDS. If a data request is made for a request that has not been developed, the requester is required to fill out a Project Intake Form (available at www.CHORDSNetwork.org). After evaluation of the Project Intake Form by the Project Development Work Group, each new public health request will be brought to the Governance Committee. Members will vote on whether to approve the development of new public health requests.

2. Research
Researchers who wish to use CHORDS data should contact the Project Manager for Research (PMR) or a member of the Research Council. After evaluation by the Research Council, each research request will be brought to the Governance Committee by the Research Council. Members of the Governance Committee will vote on all research requests. Each research project needs to comply with research regulatory requirements such as executing data agreements, obtaining Institutional Review Board (IRB) approval or non-human subjects research designation, and any other institutional approvals required by individual data partners. When necessary for grant writing or assessing feasibility of a project, preparatory to research requests can be completed using CHORDS data after project approval by the Governance Committee (or Executive Committee if so delegated).

H. Participation of Principal Investigators (PIs) and Data Partners in Scientific Proposals and Projects
In order to support research projects using CHORDS, each data partner may identify a Site PI who will represent his or her site on the Research Council. Each Site PI is responsible for internal site review of potential projects and for final decisions regarding participation in each project. Site PIs for data partners who decide to participate in a specific research project will work closely with that project's designated PI.

Each data partner reserves the right to opt in or to opt out of any research project at any time. Reasons why a data partner decides to opt out should generally be disclosed to the project's PI or a member of the Executive Committee.

IV. Data Infrastructure and Governance

Data partners use different EHR vendors and different clinical, administrative, and patient data-access applications to support clinical care and to collect patient data. Institutional differences in configurations, workflows, operational impact on real-time systems, and codes prevent sharing data directly from existing systems, even among partners using the same EHR product.

The approach chosen by CHORDS to resolve these barriers to multi-institutional data sharing is to require that data partners adhere to a common data model, which provides unambiguous definitions for structuring each data element and assigning codes to data values.

CHORDS adapted its data model, the Virtual Data Warehouse (VDW), from the Health Care Systems Research Network (HCSRN) (formerly HMO Research Network). Data governance principles have been adapted for CHORDS from prior scientific networks including the Patient Outcomes Research to Advance Learning (PORTAL) Network and the Scalable Partnering Network (SPAN) for Comparative Effectiveness Research. CHORDS continues to expand the scope and depth of the CHORDS VDW as described in Section IV.B.

A. Distributed Data Approach

CHORDS uses a distributed data approach in which data partners maintain physical and operational control over their electronic data. Data partners and data users are responsible for proper stewardship of CHORDS data in their possession.

Governance principles for distributed data include:

- Data partners retain full physical and operational control over the content and availability of their patient-level and local organizations' data.
- Results documents containing protected health information are not shared outside of the CHORDS Network with data users for public health purposes. Sharing data that are not fully de-identified (data that are part of a limited data set) for public health purposes, while allowable under the HIPAA Privacy Rule, would require more detailed data sharing agreements that follow data partner sites' regulatory requirements.
- Sharing patient-level records for public health purposes may require further IRB clarification and institutional approval, as well as appropriate data sharing agreements. (See Appendix B.)
- Each site has the right to opt in or opt out of requests to share health data, including counts and/or patient-level records for research purposes. Researchers must also obtain IRB approval or a non-human subject research designation, as well as appropriate data sharing agreements for each participating site.
- For research studies, researchers must agree that they will limit their use of the data to the purpose(s) stated in the research plan approved by the Research Council and Governance Committee. They must also identify a data storage and destruction plan for any data obtained from CHORDS. This plan must be included in the application submitted for IRB approval. Misuse of CHORDS data will result in 1) termination of access to CHORDS data, 2) report of misuse to the study's IRB and 3) any additional consequences as outlined in study-specific DUAs.
- For research studies, all research personnel who will work with CHORDS datasets must be identified in the study's IRB application and must have successfully completed IRB and HIPAA trainings as required by their home institution.

- Participation in projects requires adequate resources for the work requested.
- Data partners have the right to determine if they will participate in a specific data request.
- Data partners must have a minimum level of participation in CHORDS requests to be considered active contributors. Data partners who do not maintain active participation in responding to requests will be evaluated as described in section III.D.

The CHORDS PopMedNet (PMN) application is used to query network data (make a "request") that meet specified clinical or demographic criteria. Results come from data partners who supply data from their institutional databases stored in their local instances of the CHORDS VDW (format described below). Each data partner establishes its internal processes for determining whether the Data Mart Client (DMC) Administrator executes the request on the local CHORDS VDW instance and whether to release the data back to the requestor.

A CHORDS Data Mart consists of: (a) a database of the data partner's clinical information that has been transformed and loaded into the CHORDS VDW (see Section IV.B), and (b) a user interface, the DMC program, used by the data partner's DMC Administrator for gatekeeping decisions.

CORHIO – which hosts CHORDS' PMN Portal application – is responsible for providing a secure environment for this instance. Any significant changes to CHORDS' PMN application will run through CORHIO's existing change management processes. Minor changes and updates will be handled directly between CORHIO and developers at ACCORDS.

B. CHORDS Virtual Data Warehouse

Each participating CHORDS data partner institution will maintain a Data Mart that can be queried according to governance specifications. The structure and content of each Data Mart is based on the CHORDS VDW.

The full scope of the CHORDS VDW is explained in the CHORDS VDW Data Model Manual (available upon request). At the core of the CHORDS VDW are standardized tables and definitions. A data dictionary specifies the common format for each table and metadata about its data elements, e.g., variable name, variable label, code values. Data partner programmers have mapped and transformed data elements from their local EHR systems to the common CHORDS VDW standards.

All tables in a data partner's Data Mart are linked by a locally-generated, anonymized CHORDS PERSON_ID. No direct identifiers of individuals can be returned in a request that is distributed to a public health data user. The crosswalk between a data partner's patient and randomly generated identifier ***is never shared***.

The same principles apply to the CORHIO-assigned identifier which is used to create de-duplicated aggregate datasets and to merge across sites for longitudinal analysis when approved. The identifier is not released to public health users. Approved studies may require crosswalks between the identifier and the anonymized patient identifier, but those crosswalks are never shared.

Governance principles regarding CHORDS common data model include:

- The Governance Committee, with support from the Data Work Group, will identify and prioritize changes to the CHORDS VDW that will be implemented on an annual basis.
- Data partners will implement all tables and attributes identified in the data dictionary and populate with data as many as is feasible.
- Data partners will implement CHORDS VDW changes to the best of their ability, balancing time and budget constraints.

- Data partners are responsible for maintaining and updating data extracts with data refreshes at least quarterly.
- Data partners, with support from the Data Work Group, are responsible for data QA and resolution of data quality issues.

C. Data Requests and Data Exchange

CHORDS data requests and data exchange are managed by the PMN application, a software which is used by multiple national networks such as the Federal Drug Administration Mini-Sentinel Initiative and the Patient-Centered Outcomes Research Institute (PCORI)-funded Patient Centered Outcomes for Research Network (PCORnet). PMN provides security, authentication and auditing required to ensure that only approved data requests are made. All CHORDS data partners will install the PMN DMC for responding to requests.

The CHORDS network consists of a single query portal for making federated queries that is connected to multiple Data Marts through a PMN client installed at each data partner for responding to federated queries. The CHORDS VDW query portal, hosted at CORHIO, includes an authorization and authentication (unique logon and password for users) infrastructure and is maintained by the Network Operations Work Group. Authorized data users may access the query portal to pose queries to the network and retrieve results.

Governance principles for all CHORDS data queries and data exchange include:

- All data requests must identify the requesting organization, responsible individual and contact information and intended use(s).
- Data partners will identify a technical contact (if separate from the DMC Administrator, see Appendix E.) who is responsible for ensuring timely approval and execution of requests.
- Approving, executing and releasing data should be completed within two weeks of receiving a request. Data users may contact data partners to request an expedited process, if necessary.
- Data partners will store the CORHIO-assigned identifiers in their CHORDS VDWs and share those in response to a public health or approved research request that requires de-duplication or linkage of patient records. The identifier may not be shared in any other way nor may it be used for any other internal or external purpose.
- Data partners may decline to respond to requests or decline to release request results upon query execution.
- Data partners will review requests prior to execution.
- Data partners will review results prior to release.
- Data queries and exchange will adhere to the CHORDS policy of not releasing to the public aggregated cell sizes less than or equal to 10.

Some principles governing data requests and data exchange vary based on the data user.

1. Public Health
    - Data requests will never include identifiable patient or site/data partner identifiers.
    - When request results have been de-duplicated across sites, data users will receive only final, aggregated results and will not have access to any intermediate information related to the CORHIO-assigned identifier.
    - Data requests will be sent to all data partners, who may choose to run them.
    - Data users should limit the frequency of their requests to minimize the burden placed on CHORDS data partners. If necessary, CHORDS Project Managers for Research and/or Public Health will establish a suggested maximum frequency.
    - Aggregate results must be stored in a secure manner and may be retained as long as needed.

- Query metadata (e.g. date of data request, filter settings, number of responses received, number of sites declining request, etc.) will not be separated from query results.
- Data users will adhere to recommendations about insufficient data. While included in the aggregate results (if >10), cells not meeting sufficient data criteria should not be used externally.
- Designated data users at LPHAs are responsible for ensuring that other LPHA staff use CHORDS results responsibly and accurately.

2. Researchers

- Data requests and data exchange may include protected health information (PHI). Any use of PHI for research must be approved by Colorado Multiple Institutional Review Board (COMIRB) or other IRB and agreed to by all participating sites by these sites entering into the appropriate data sharing agreement. Data requests and data exchange will never include site/data partner identifiers unless explicitly requested by the researcher, agreed to by data partners and stipulated in the data sharing agreement.
- Data requests will be sent only to data partners who have agreed to participate in a given study.
- All CHORDS results must be stored in a secure manner. Data storage and data destruction plans must be provided by the researcher and receive IRB and CHORDS approval.
- When sharing results, query metadata will not be separated from query results.
- For studies using aggregated data, researchers will adhere to recommendations about insufficient data. While included in the aggregate results, cells not meeting sufficient data criteria should not be used externally.
- Researchers are responsible for ensuring that all dissemination of research using CHORDS data is done responsibly, accurately and with appropriate attribution and acknowledgement.
- For research studies, researchers must agree that they will limit their use of the data to the purpose(s) stated in the research plan approved by the Governance Committee. Researchers also agree to not re-distribute data to individuals not listed as study personnel in their IRB applications. See the Governance Principles section above for additional details on consequences of data misuse. Any amendments to the use of the data will be reviewed by the Governance Committee and must be approved prior to implementation.
- Research requests that seek to use the CHORDS identifier in their studies must be approved by the CHORDS network including CORHIO. The CHORDS identifier assigned by CORHIO (using clear text exchange with that entity) is specific to CHORDS. Although derived using the same tools and software, it is different than any CORHIO identifier used for other state-wide identity management activities.
- In addition to the primary approach used in CHORDS (the CORHIO-assigned identifier), there are a number of other techniques for assigning unique identifiers to individuals represented in multiple systems that researchers may opt to utilize. Researchers may be required to use non-clear text linkage techniques. A particular category of techniques, known as Privacy Preserving Record Linkage (PPRL), has advantages for academic research in some instances. PPRL reduces the amount of identifiable information shared outside of an organization's firewall, with a potential for decreased matching accuracy due to less comprehensive PHI used for matching. Other identifiers may be generated for research requests using PPRL (or other) techniques, once approved by the CHORDS network, participating data partners and an IRB, as applicable.
- Approved research may use study-specific identifiers that are not PHI. ACCORDS at the University of Colorado will maintain these cross-walks.

D. Ensuring Data Consistency and Quality

CHORDS relies on consistent, quality data to produce valid, reliable information. Data partners agree to ensure the quality of CHORDS VDW data and the accuracy of the Extract, Transform, and Load (ETL) program that extracts data

from source systems, transforms data to conform to the CHORDS VDW specifications, and loads data into the partner's CHORDS VDW data mart.

Governance principles regarding data consistency and quality include:

- Data QA and improvement is a shared responsibility. The data partner has the lead role, supported by the Data Work Group. The data partner will take primary responsibility for executing data QA programs and for investigating data quality issues that are detected at the site and network levels. The Data Work Group develops and shares data quality tools within the PMN client.
- Each data partner is responsible for refreshing data on at least a quarterly basis and for staying aligned with CHORDS updates as time and resources allow.
- Each data partner is responsible for completing site-specific QA checks after each data refresh or change to the CHORDS VDW.
- When a significant data quality issue is discovered, the data partner will take the lead in informing the Data Work Group, identifying the source and developing solutions.

E. Data Access

Access to data exchange software through CHORDS is limited to specific roles in PMN™. These roles are described in Appendix E.

Requesting data access for public health purposes involves the following steps:

- The public health director, or designee, works with the CHI or current governance convener to execute data use agreements with data partners as needed.
- Upon executing data use agreements, the public health director, or designee, identifies a staff member to serve as the agency's authorized CHORDS user. The director, or designee, includes the data users' contact information in a signed CHORDS User Access Form (see Appendix C), which is sent to the chairs of the Network Operations Work Group for verification and to create a PMN account for the public health data user.
- The public health data user works with the Network Operations Work Group to set up a PMN tutorial and to review CHORDS policies and guidelines.
- Public health data users may submit requests after data use agreements and User Access Forms are signed and necessary training is received. Data users may only use CHORDS data for purposes that align with public health purposes outlined in the data use agreements.

Requesting data access for research purposes involves the following steps:

- The research Principal Investigator (PI) contacts the Project Manager for Research (PMR) or another member of the Research Council with a proposed research question. The research PI completes the CHORDS Project Intake form.
- The PMR and the Research Council will perform an initial assessment of the request based on fit, feasibility, and funding opportunities.
- If the Research Council supports the project moving forward, the project will be brought to the Governance Committee for review and final approval. Approval is required for all -requests before any prep-to-research (PTR) or other data requests are initiated.
- After Governance Committee approval, PTR data requests may be completed.
- The PI will apply for IRB approval/non-human subject research designation.
- The PMR will work with data partners to identify which sites will participate in a given project.
- The PI will work with the Governance Committee and data partners to execute the necessary data agreements.
- The PI will complete the required CHORDS access forms and tutorials (see above under public health).

- PIs initiate queries, or works in partnership with a CHORDS developer, when data use agreements are signed, after receiving necessary training, and in partnership with the PMR or a representative of the Research Council.
- Researchers must limit their use of the data to the purpose(s) stated in the research plan approved by the Governance Committee.

CHORDS strives to identify viable, feasible projects before submitting any data requests to our data partners. Several stages of screening may be required in selecting appropriate and feasible research projects.

Note on Preparatory to Research (PTR) data requests:

Preparatory to research (PTR) queries of CHORDS do not require IRB review, although individual institutions may require other forms of pre-review. HIPAA requirements that govern the access to PHI for PTR activities are operationalized at the institutional level. As with any data request, data partners may choose to opt out of any PTR request.

In the case of a CHORDS PTR query where simple counts are returned to the requestor, no PHI is shared. The Governance Committee views it as consistent with HIPAA to not require any specific action for PTR queries. Researchers interested in executing a PTR query may contact the PMR or Research Council.

If a data partner's local institution requires a different process for PTR queries, the researcher must work with that data partner and the PMR in order to ensure that the site's needs are met before completing a PTR request. Please note that the Data Mart Administrator has the opportunity to review every request prior to executing it and sharing results.

Research requests must be vetted by the PMR, the Research Council, and approved by the Committee before any PTR data requests are completed.

F. Data Use Limitations

Data partners may use their own source data stored in the CHORDS VDW for other purposes, including research, as long as they comply with applicable state and federal laws and regulations, including HIPAA and the Common Rule, and undergo local review processes.

Data users may only use data obtained from CHORDS for purposes identified in the data use agreements. Data may not be reused, disclosed, altered, or sold for any purposes other than those defined in the agreements.

Note on Creating De-Duplicated Public Health Estimates

The CHORDS Network is originating a two-step process that securely removes duplicate individuals from distributed public health queries' prevalence estimates while maintaining its commitment to exchanging the minimum data necessary.

Data partners work with CORHIO to assign identifiers to their patients by exchanging record-level data outside the CHORDS infrastructure through a secure file transfer protocol (SFTP) site.

Data partners may only use the identifier that is provided by CORHIO and stored in the CHORDS VDW to facilitate the creation of de-duplicated, public health estimates for the CHORDS Network. Any other use of the CORHIO-assigned identifier, including CHORDS-related research, must receive prior approval by the CHORDS network that includes CORHIO.

See Appendix F for more information.

V. Security, Privacy and Confidentiality

All CHORDS Network members are charged with responsible stewardship of patient data by maintaining, and strengthening when possible, the privacy and confidentiality of patient data. The CHORDS Network believes that the protection of privacy, confidentiality, and data security is essential to the existence and success of public health monitoring and research.

The HIPAA Privacy and Security Rules establish minimum federal standards for protecting privacy and maintaining confidentiality of PHI. In the context of CHORDS these responsibilities begin with the data partner organizations and extend, through formalized relationships based on federal law, between the data users, Executive Committee, Advisory Council and Work Groups.

The IRB of record for CHORDS is COMIRB and any additional IRBs as appropriate for the data partner organizations. COMIRB has reviewed the CHORDS infrastructure and declared its public health uses not human subject research.

COMIRB has also approved the CHORDS infrastructure for research uses. Each research study using CHORDS must apply for its own IRB approval (e.g., describing study's procedures, data handling, and intended use of the data) which may reference CHORDS' prior review by COMIRB.

If CHORDS data are released, shared, and/or accessed in a way that is inconsistent with processes approved by the IRB of record, collaborating IRBs and executed data use agreements, the procedures in Appendix G., Data Incident Response Plan, will be followed. These procedures include timely and transparent communication regarding the disclosure with the data partners and the Governance Committee. CHORDS staff will also communicate any data incidents to the appropriate HIPAA officials at the University of Colorado Anschutz Medical Campus and collaborating organizations in accordance with University policy. CHORDS staff and the Committee will cooperate with and assist the University's HIPAA Compliance officers in their Incident Response and Reporting Process.

A. Security

Privacy and confidentiality of electronic data depend on control over access. Secure access consists of deterring unwanted access and authorizing only specific types of access to authenticated individuals.

Security functionality depends on PMN, which securely protects data for several national and federally funded efforts. PMN design provides secure, compliant, auditable data transfer.

Public health users must complete the CHORDS onboarding process. This includes identifying users. (In the early stages of CHORDS expansion, each public health agency will have one approved user. The number of approved data users per site may change in the future.)

Researchers must also complete the CHORDS onboarding process. This includes identifying all study personnel who will work with CHORDS data and specifying those that will log into CHORDS to request and access datasets.

All users must complete a User Access Form before receiving account approval. Users must also complete CHORDS/PMN training.

B. Privacy & Confidentiality

The Privacy Rule permits assigning a code or other identification to a patient's health information that protects the person's identity. Data partners and data users may not use or disclose the code and may not disclose its method of identifying the information.

The Security Rule addresses the technical and non-technical safeguards that organizations must have to protect the privacy of individuals' PHI.

CHORDS takes a number of steps to limit risks to privacy.

- The only data to be released based on a public health query request must meet small-cell guidelines (cells containing 10 or fewer individuals are masked).
- Data are shared in aggregate or as a limited dataset to remove identifying information such as patient names, addresses and phone numbers.
- Data partners may only use the CORHIO-assigned network-wide identifier to complete PMN instructions for de-duplicating public health requests for CHORDS requests only.
- The CORHIO-assigned identifier stored in data partners' CHORDS VDWs is not, and does not contain, PHI. CORHIO will maintain a cross-walk in its environment between the unique identifier that is PHI and the identifier that is provided to data partners.
- For research requiring access to patient-level data, only limited dataset information is available and will only be shared when the required IRB approval(s) and data sharing agreement(s) are in place. Attempts to re-identify patients are not permitted and will be treated as incidents requiring investigation with the Data Incident Response Plan previously described.
- Access to CHORDS is permitted only to users who have permission from the Governance Committee to access the data network and have signed data agreements. Each time a user accesses the network, he/she must identify themselves through user authentication (providing a username and password), and a record of access is kept.
- CHORDS has written documentation of its HIPAA compliance policies and procedures to ensure proper use and storage of data by all users.
- Data are never attributed to a site nor are data from one partner site compared with data from another unless sites have provided written consent and approval.

VI. Publication and Presentations Guidelines

Each CHORDS data partner has complete control over the use and confidentiality of its data. By providing data for public health uses, data partners are agreeing for their data to be used publicly, in accordance with data agreements and CHORDS principles and guidelines.

A presentation or publication (whether in popular press or an academic journal) including CHORDS data from multiple CHORDS data partners will generally have at least one co-author or acknowledged contributor from each site. Co-authorship implies that the data partner is responsible for the quality and integrity of its data and working with users on its interpretation and meets the requirements of co-authorship per International Committee of Medical Journal Editors (ICMJE) guidelines: http://www.icmje.org/recommendations/browse/roles-and-responsibilities/defining-the-role-of-authors-and-contributors.html. Contributors review and provide feedback on manuscript drafts, but may be less involved in the planning, execution and analysis of the research project and/or data.

Review and Comment by Co-Authors and Contributors:

An author must submit a draft manuscript, abstract or presentation (online or in-person) based on CHORDS data to each data partner supplying data for the study (or a designated committee) for review and comment. Each data partner (or the designated body) will review the manuscript within 30 days or less. CHORDS Project Managers for

Research or Public Health must also review these drafts before submission or publication to ensure CHORDS is referenced accurately. Authors are responsible for allowing sufficient and reasonable time for review by all parties.

Blinding Source of Data in Publications and External Communications:
Joint Studies: A publication or other external communication resulting from a joint research study may not include identifying information of participating data partners without the permission of that site. Such publications or other external communications do not need to be presented in aggregated form, but a data partner may object to the presentation of the non-aggregated information if the data partner believes the information could be used to identify the site.

Single-Member Studies: Except as related to joint studies as specified above, a publication or other external communication related to use of data may not include the name, location and other geographic data, ranking, or confidential information of a site, without consent of that site.

Acknowledgments: Each data partner and data user agree to acknowledge CHORDS and use of CHORDS data in any work based in whole or part on any data received through CHORDS, and to acknowledge the organizations that provided funding for CHORDS. CHORDS project managers can provide appropriate citation information. An author takes full and final responsibility for his or her analysis of CHORDS data and the presentation of any analyses or conclusions in any publication or presentation.

VII. Research Conflicts of Interest
Project data will only be accessible to CHORDS investigators and approved nonaffiliated investigators whose home institutions maintain and enforce Conflict of Interest (COI) policies for staff investigators. These policies must address employees and their immediate family members. For research activities, investigators must also comply with COMIRB's COI policies.

CHORDS relies on the investigator's home institution to maintain an appropriate written, enforced policy on COI that complies with Federal Regulation 42 CFR 50 Subpart F: Responsibility of Applicants for Promoting Objectivity in Research for Which PHS Funding Is Sought. Participating institutions are expected to have COI policies that meet these minimum standards. It is expected that CHORDS investigators and approved non-affiliated investigators who have access to project data, abide by the policies of their home institution. These must include, at a minimum:

- Processes to determine COI;
- Requirements to disclose financial interests (including those of immediate family members) that might pose COI or perceived COI;
- Requirements to disclose COI that might affect the research process or study participants, including situations in which the investigator may have a real or perceived undue influence over the research process;
- Remedies to manage, reduce or eliminate the COI or the appearance of COI
- Enforcement mechanisms that impose sanctions when appropriate.

VIII. Scientific Misconduct
The CHORDS Governance Committee must be informed of any scientific misconduct by the site PI from which the misconduct originated. These instances are expected to be addressed by the investigator's home institution and issues and resolution communicated to the Governance Committee and data partners. The Governance Committee may decide to take action based on the reported scientific misconduct activity.

IX. Glossary

- **Adapter –** a group of pre-defined structured data requests on a specific topic. For example, CHORDS has a Mental Health adapter that contains diagnosis-specific requests (e.g., depression, schizophrenia or anxiety).

- **CHORDS Portal** – the web application component of the PopMedNet system. There is one CHORDS Portal, hosted by the Adult and Child Consortium for Health Outcomes Research and Delivery Science. Investigators log in to the CHORDS Portal to submit their data queries. The Data Mart Client at each site accesses these requests and returns data to the Portal. The Portal aggregates data across sites; investigators log in to the Portal to access their result files.

- **Data Governance** – strategies that define the structure, format and purpose for collecting data.

- **Data Mart Client (DMC) –** the software application component of PopMedNet that is installed by each data partner. The DMC connects the site's CHORDS VDW to the CHORDS network. The DMC polls the central CHORDS Portal for any waiting requests and is used to execute those requests against the site's Virtual Data Warehouse. The DMC is then used to return results to the central CHORDS Portal for aggregation and sharing with the data user.

- **Data Partner** – A health care or mental health provider that establishes a connection between a virtual data warehouse and the CHORDS network using PopMedNet.

- **Data Standard*** – a predetermined set of structural and semantic data requirements for each CHORDS Virtual Data Warehouse.

- **Data Stewardship** – using data accessed through CHORDS according to the established governance plan.

- **Data Use Agreement (DUA)** – a contract concerning the transfer of non-public data. A DUA outlines the terms and conditions of the data transfer, including limitations on its use and required procedures for keeping data secure.

- **De-identified Data Set**** – data that have been stripped of all protected health information identifiers. De-identified data sets are not considered protected health information. According to the Health Insurance Portability and Accountability Act (HIPAA), covered entities may use or disclose health information that is de-identified without restriction under the Privacy Rule. Covered entities seeking to release this health information must determine that the information has been de-identified using either statistical verification of de-identification or by removing certain pieces of information from each record as specified in the Rule. The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements (see below) that could be used to identify the individual or the individual's relatives, employers or household members. The covered entity also must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information.

  Under this method, the identifiers that must be removed are the following:
  1. Names.
  2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
     a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.

   b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic or code, unless otherwise permitted by the Privacy Rule for reidentification.

- **Identifier** – a person-specific identifier for the CHORDS Network that is consistent across multiple data partners

- **Limited Data Set (LDS)**** – protected health information that excludes certain direct patient identifiers. According to the HIPAA Privacy Rule, an LDS may be used for research, public health, or health care operations when the data set recipient enters into DUA with the site (data owner) providing the data set.

  An LDS can include dates, limited geographic information and a link field (e.g., an encrypted identifier), such as:
  - Dates (e.g., admission, discharge and service dates; dates of birth and death) and ages of research participants;
  - Certain general geographic information, including five or nine-digit zip codes and state, county, city and precinct; and
  - Links which may be used to identify individuals when the researcher maintains and holds confidential the key required for reidentification.

  An LDS must exclude all other protected health information identifiers, such as:
  - Names and street or postal addresses;
  - Telephone and fax numbers;
  - E-mail and Internet Protocol (IP) addresses and web Universal Resource Locators (URL);
  - Social Security, medical record, health plan beneficiary and other account numbers;
  - Certificate and license numbers;
  - Vehicle identifiers and serial numbers, including license plate numbers;

- Device identifiers and serial numbers;
- Biometric identifiers, including finger and voice prints; and
- Full-face photos and any other comparable images.

- **Process Standard*** – format, language and content of queries, data models and processes that affect CHORDS operations.

- **Protected Health Information** (PHI) - individually identifiable health information.

- **Request** – a pre-defined structured data request that falls under an adapter on a specific topic. For example, a diagnosed depression request would fall under the Mental Health adapter.
- **Technical Partner** - organizations that provide services to catalog, curate, manage or improve data from data partners.

- **Virtual Data Warehouse (VDW)** – a database containing data extracted directly from a local electronic health record that is reconfigured using standard variable names and values. Each CHORDS data contributor establishes its own VDW, allowing CHORDS to produce comparable data that can be easily merged across sites in order to conduct public health monitoring and other research.

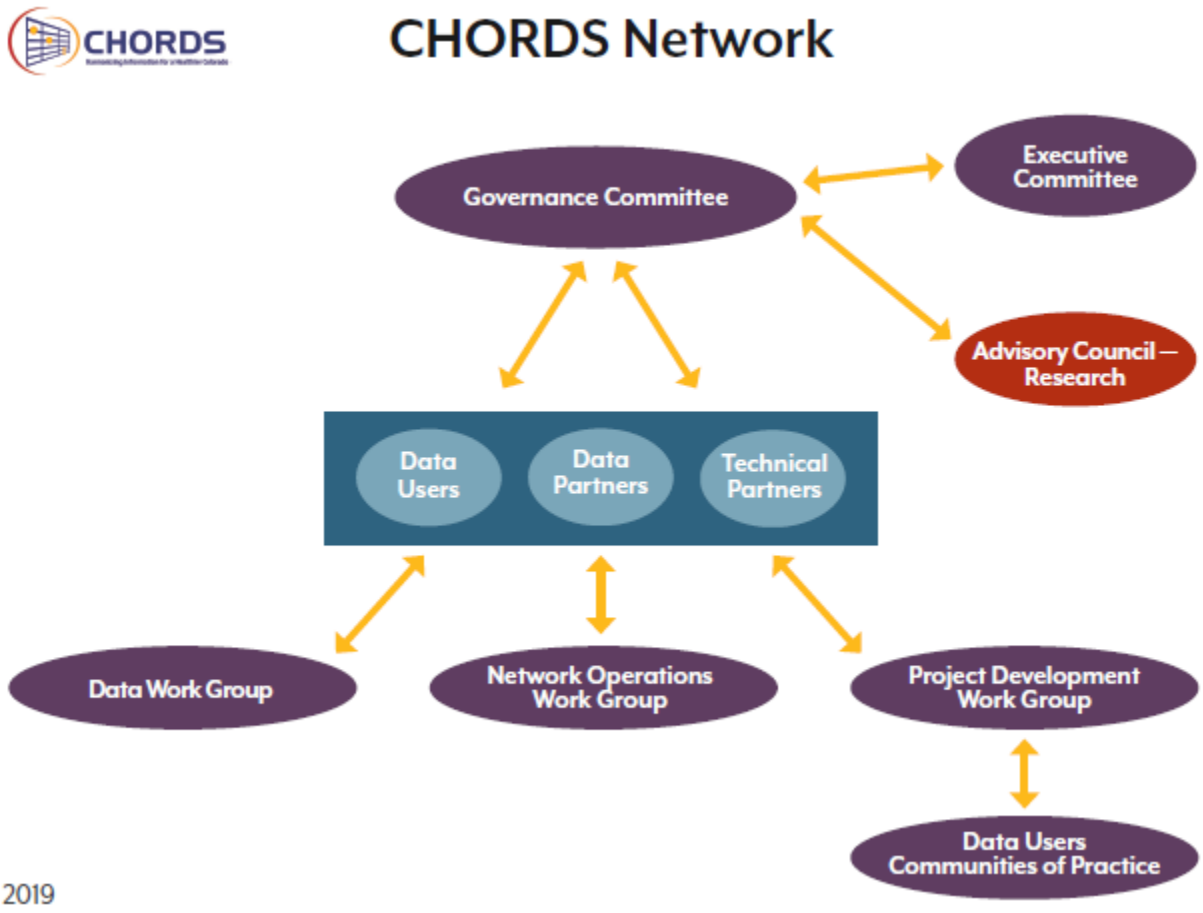
*Definitions for these terms are drawn from Holmes JH, Elliott TE, Brown JS, et al. *J Am Med Inform Assoc.* 2014; 21:730–736.

**Definitions for these terms are from the Governance of the Patient Outcomes Research to Advance Learning (PORTAL) Network, Version 3 November 2015. Authors: Steiner JF, Nelson AF, Paolino AR, McGlynn E.

XII. Appendix

A. CHORDS Network Structure
B. Data Use Agreement Template
C. CHORDS User Access Form
D. Work Group and Council Charters
E. CHORDS Roles and Settings
F. CHORDS Identity Management
G. Data Incident and Response Plan
H. Memorandum of Understanding Template

Appendix A. CHORDS Network Structure



Appendix B. Data Use Agreement Template

DATA USE AGREEMENT

This Data Use Agreement ("Agreement") is entered into by and between _____ (hereinafter, "Covered Entity") and the Data Recipients named in Schedule 1 (attached hereto and incorporated herein by reference) (each a "Data Recipient" and collectively the "Data Recipients"). Covered Entity and each Data Recipient may herein be individually referred to as a "Party" or collectively as the "Parties".

RECITALS:

WHEREAS, the Parties are committed to improving the health of the populations and the communities they serve;

WHEREAS, Covered Entity is providing to each Data Recipient the data described in Schedule 1, which contains certain Protected Health Information in the form of a Limited Data Set (hereinafter referred to as the "Data") for the purposes of research or public health as described herein; and

WHEREAS, this Agreement addresses the conditions under which Covered Entity will disclose and the Data Recipient may obtain, use, reuse, and disclose the Data in accordance with Applicable Law;

NOW, THEREFORE, in consideration of the mutual promises and considerations set forth below, the Parties agree as follows:

1. **Definitions**. Any capitalized terms used in this Agreement and not otherwise defined, shall have the meanings set forth in the HIPAA Privacy Rule, which definitions are incorporated in this Agreement by reference.
    a. "Applicable Law" means HIPAA, the HITECH Act, and all the regulations promulgated thereunder, as well as any other applicable federal, state, or local law.
    b. "Data Use Agreement" shall have the same meaning as specified in the standards in 45 CFR Section 164.514(e)(4).
    c. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-005, and the regulations promulgated thereunder by the U.S. Department of Health and Human Services and its Office of Civil Rights.
    d. "Limited Data Set" shall have the same meaning as specified in the standards in 45 CFR Section 164.514(e).
    e. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, Subparts A and E.
    f. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 CFR Section 160.103.

2. **Term**. This Agreement shall commence on the Effective Date set forth in Schedule 1 and shall continue in effect until terminated in accordance with Section 4 below. To the extent that a Data Recipient is added to this Agreement after the Effective Date, then the Effective Date of the Agreement as to the later added Data Recipient shall commence on the date of execution with Covered Entity.

3. **Data Recipient's Obligations.**

    a. **Permitted Data Use.** Data Recipient shall only receive, use or disclose the Data for the purposes described in Schedule 1 and shall not use or further disclose the Data unless otherwise required by law, or as authorized by Covered Entity in writing.

    b. **Safeguards.** Data Recipient shall use appropriate safeguards as required by Applicable Law to prevent any use and disclosure of the Data, other than as provided for by this Agreement. Upon request by Covered Entity, Data Recipient shall describe the safeguards being used to prevent unauthorized use or disclosure of the Data.

    c. **Reporting Unauthorized Use or Disclosure.** Data Recipient shall immediately report to the Covered Entity any use or disclosure of the Data other than as expressly allowed by this Agreement of which Data Recipient becomes aware. Unauthorized uses or disclosures of the Data by Data Recipient is grounds for termination of this Agreement by Covered Entity in accordance with Section 4.

    d. **Data Recipient Workforce**. Data Recipient shall ensure that its employees, representatives, and agents each agree to comply with the terms and conditions of this Agreement, and shall ensure that its agents, Business Associates and subcontractors to whom Data Recipient provides the Data each agree to comply with the same restrictions and conditions that apply to Data Recipient hereunder.

    e. **No Identification of Individuals.** Data Recipient shall not identify or attempt to identify the information contained in the Data, nor contact any of the individuals whose information is contained in the Data.

4. **Termination**.

    a. For Cause. Covered Entity may terminate this Agreement with respect to one or more Data Recipient(s) and cease all disclosures of Data pursuant hereto, upon ten (10) days' notice to Data Recipient(s) if Data Recipient(s) violates or breaches any material term or condition of this agreement.

    b. Covered Entity or Data Recipient may terminate this Agreement for any reason upon 30 days' written notice to the other Party.

    c. Upon termination of this Agreement by either Party or upon completion of Data Recipient's purpose for requesting the Data identified on Schedule 1, whichever occurs first, Data Recipient shall promptly return or destroy the Data using industry-accepted methods. If return or destruction of the Data is not feasible, Data Recipient shall continue the protections required under this Agreement consistent with the requirements of the Privacy Rule.

5. **Interpretation.** Any ambiguity in this Agreement relating to the use and disclosure of the Data by Recipient(s) shall be resolved in favor of a meaning that further protects the privacy and security of the Data.

6. **Liability.** Except as expressly set forth herein, the Parties acknowledge and agree that each Party will be responsible for its own acts, errors, omissions, or the results thereof to the extent permitted by Applicable Law and shall not be responsible for the acts, errors, omissions, or the results thereof of the other.

7. **Amendment.**
    a. Any amendment to this Agreement must be made in writing, signed by the Parties, except that Schedule 1 may be modified or amended by agreement of the Parties in writing from time to time without formal amendment of this Agreement.
    b. Addition of Data Recipients. Covered Entity may agree to provide the Data to a new data recipient upon execution of this Agreement by the Covered Entity and the new Data Recipient and amendment of the Data Recipient list in Schedule 1. The addition of new Data Recipients shall not affect the rights or obligations of then existing Data Recipients in any way.
8. **Compliance with Laws.** Each Party represents and warrants that it will at all times comply with Applicable Law in the performance of this Agreement.
9. **Counterparts**. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.
10. **Entire Agreement.** This Agreement is the complete agreement between the Parties and supersedes all previous agreements or representations, written or oral, with respect to the Data and any related matters as addressed herein.
11. **Notices.** Any and all notices required or permitted under this Agreement must be in writing and sent by United States mail, electronic mail with written acknowledgement of receipt, overnight delivery service or facsimile to the addresses for each party provided below or such different address as a party may later designate in writing.
12. **Independent Contractors.** The relationship between the Parties is that of independent contractors. This Agreement will not create any agency, joint venture, or partnership relationship between the Parties.
13. **Severability.** In the event any part or parts of this Agreement are held to be unenforceable, the remainder of this Agreement shall continue in effect.

IN WITNESS WHEREOF, the Parties have executed this Agreement as follows:

COVERED ENTITY
Name

By_____

Name

Title

DATA RECIPIENT
Name:

By_____
Name:
Title:

Schedule 1

1. Effective Date:

2. Name of Covered Entity contact person/department releasing the Data:

3. Name and Contact Information of Data Recipients:

Data Recipient	Address	Workforce

4. Purpose of Data disclosure: Data Recipient may use and disclose the Data for public health surveillance activities of the following conditions:
   - Infectious or communicable diseases.
   - Chronic diseases, conditions or health behaviors.
   - Behavioral health conditions.

5. Each Data Recipient is permitted to use and disclose the Data for the following specific purpose(s):

   Covered Entity's Data may be combined with data from other regional collaborators to create a Consolidated Data Set (CDS). The CDS will be used to monitor population health, target areas for intervention and conduct evaluation activities. Analyses conducted on the CDS data will be shared on a regional basis in accordance with this Agreement and with the goal of improving health and the quality and availability of health care and health resources in neighborhoods or sub-

county regions. Reports developed from the Data and CDS may be disclosed at the county, council district, neighborhood level or census tract in accordance with the purpose described above.

6. Description of Data elements disclosed for the public health purposes described in Sections 4 and 5.

Public health surveillance data related to the conditions described above in Section 4 for the year 2000 and forward. Data elements are described in the current CHORDS VDW Data Model Manual and are based on the Virtual Data Warehouse [VDW] (a database containing data extracted directly from Covered Entity's EHR that is reconfigured using standard variable names and values).

Covered Entity will generate, assign and store a unique identifier for patients, providers and encounters that will be used to join health information across tables.

In order to qualify as a Limited Data Set under HIPAA and this Agreement, the Data must exclude the following direct identifiers:

a. Names
b. Postal address information, other than town or city, state, and zip code
c. Telephone numbers
d. Fax numbers
e. Electronic mail addresses
f. Social Security numbers
g. Medical record numbers
h. Health plan beneficiary numbers
i. Account numbers
j. Certificate/license numbers
k. Vehicle identifiers and serial numbers, including license plate numbers
l. Device identifiers and serial numbers
m. Web Universal Resource Locators (URLs)
n. Internet Protocol (IP) address numbers
o. Biometric identifiers, including finger and voice prints, and
p. Full face photographic images and any comparable images.

Appendix C. CHORDS User Access Request Form

1. By signing, I agree that I have read, understand and will abide by the CHORDS Data Use Agreement
2. Fill in the information below, print and sign where indicated, obtain your manager/supervisors signature and submit to: Rachel Zucker/Jessica Bondy/Bryant Doyle, email: CHORDS.Support@ucdenver.edu

By signing, I agree to use CHORDS only for work-related business. I will not share my account password with anyone or let others use CHORDS while I am logged in. I agree to use recommended security practices where possible, including encrypting computers used to connect to CHORDS; and physically securing computers by working in access-controlled or locked areas and using automatic screen-saver time outs. I agree to share the information obtained within CHORDS only with personnel who have a legitimate work-related need for the information. I understand failure to comply with the institution's policies and procedures may result in termination of access to CHORDS and other employment consequences depending on the nature of the violation.

Validation of work-related need for anyone requesting CHORDS access is required. If requesting access to electronic protected health information (ePHI) I attest to the need to use electronic devices that access, create, store and receive ePHI AND that the electronic devices that I use with ePHI are fully encrypted with all security provisions applied. I agree not to store any reports from CHORDS on removable hardware (ex. USB drives). I understand that information about my use of the CHORDS system is logged and that these logs are audited on a regular basis. I agree to access only the minimum necessary data required to perform my duties. I agree to immediately report any suspected policy violation to my supervisor.

DATA USER INFORMATION		
Name:		
Organization:		
Email:		
Phone:		
Title:		
Business Address:		
CHORDS Point of Contact Name:		
CHORDS Point of Contact Email:		
CHORDS Point of Contact Phone:		
AFFILIATION		
Place an 'X' next to the statement that best describes you.		I represent a healthcare organization contributing data to CHORDS
		I represent a local public health agency accessing public health information for community/population health monitoring
		I am a researcher using CHORDS for research purposes
Applicant Signature:		Date
CHORDS Point of Contact Signature:		Date

ACCORDS Representative Signature		Date

TO BE COMPLETED BY CHORDS/PopMedNet ADMINISTRATION

CHORDS/PopMedNet ACCESS ACTIVATION					
Access activation process status		User info provided to CHORDS/PopMedNet OIT Support		Date:	Initials:
		Role(s) added to Requester in CHORDS/PopMedNet		Date:	Initials:
		Requester activated		Date:	Initials:
		Role changes made		Date:	Initials:

USER ACCESS ROLES

*A CHORDS user account must be created for each individual that requires CHORDS access. Once logged in, the CHORDS user is assigned an **Access Role**. Access Roles are used for security, and define which data the user may see and which parts of CHORDS the user may access.*

CHORDS Role	
	DataMart Administrator: You will be monitoring your site's datamart client (DMC), including the queries submitted and the results returned. You represent a data contributing site
	Investigator: You are submitting one or more queries and accessing data using CHORDS. You are requesting data that is aggregated from multiple partners.
	Enhanced Investigator: You are submitting one or more queries and accessing data using CHORDS. You are requesting data that is aggregated from multiple partners. You also need to see site-specific data.

Appendix D. Work Group and Council Charters

Network Operations Work Group Charter

Overview
The Colorado Health Observation Regional Data Service (CHORDS) is a regional collaborative partnership among Colorado health care delivery systems, public health departments, the Colorado Regional Health Information Organization (CORHIO), and the University of Colorado Anschutz Medical Campus to share health data. CHORDS collects, analyzes and presents data from participating partners' electronic health records (EHRs) to monitor population health, target areas for intervention, and conduct research and evaluation activities. This charter will be reviewed as needed.

Purpose
The Network Operations Work Group is responsible for day-to-day oversight of CHORDS operations, including installing, testing, maintaining and developing CHORDS data sharing software. This group is also responsible for implementing all network access and security privileges for data partners and data users as instructed by the Governance Committee, including scheduling of technical activities and identifying necessary resources; and prompt reporting of any data privacy or security incident to the Governance Committee, affected organizations, and appropriate regulatory authorities.

The Network Operations Work Group aids new users in the onboarding process and trainings, assesses appropriate network use (frequency and nature of requests being submitted), and assists in identifying data quality issues and developing solutions. The Network Operations Work Group provides the Governance Committee with analyses of the benefits and costs of software changes and upgrades, and implements any changes the Governance Committee approves.

Membership
The Network Operations Work Group includes data partners, data users, technology partners and interested stakeholders. Membership is voluntary. The Work Group will have two chairpersons, with at least one chairperson also serving as a CHORDS Governing Board member. The chairpersons will serve as liaisons between the Governing Board and the Network Operations Work Group.

Guiding Principles
The Network Operations Work Group follows the principles outlined in the CHORDS Governance Policies and Guidelines.

Decision-making
Consensus-based decisions are preferred; however, decision-making processes will vary depending upon the issue. The Network Operations Work Group chairpersons will determine, with input from the members, whether to seek consensus or use a voting process to make decisions. The Network Operations Work Group follows the decision-making procedures outlined in the CHORDS Governance Policies and Guidelines.

Meetings
The Network Operations Work Group meets quarterly and communicates using email as needed. The chairpersons can convene a meeting in the intervening weeks if necessary to discuss time-sensitive opportunities.

Project Development Work Group Charter

Overview
The Colorado Health Observation Regional Data Service (CHORDS) is a regional collaborative partnership among Colorado health care delivery systems, public health departments, the Colorado Regional Health Information Organization (CORHIO), and the University of Colorado Anschutz Medical Campus to share health data. CHORDS collects, analyzes and presents data from participating partners' electronic health records (EHRs) to monitor population health, target areas for intervention, and conduct research and evaluation activities.

Purpose
The Project Development Work Group is responsible for fostering high-quality monitoring, evaluation, quality improvement, and research activities through CHORDS. This includes assisting users in developing their questions, assessing project feasibility and assisting the Governing Board or Executive Committee in prioritizing requests.

The Project Development Work Group develops and reviews new and existing public health and research uses; advises potential users of the system; and manages project planning and timelines. It will work with existing data users and engage new ones. The Project Development Work Group may delegate specific projects and opportunities to a Community of Practice among data users. Separate Project Development Work Groups may be convened for public health users and researchers.

Membership
The Project Development Work Group includes data partners, data users, technology partners and interested stakeholders. Membership is voluntary. The Work Group will have two chairpersons, with at least one chairperson also serving as a CHORDS Governing Board member. The chairpersons will serve as liaisons between the Governing Board and the Project Development Work Group.

Guiding Principles
The Project Development Work Group follows the principles outlined in the CHORDS Governance Policies and Guidelines.

Decision-making
Consensus-based decisions are preferred; however, decision-making processes will vary depending upon the issue. The Project Development Work Group chairpersons will determine, with input from the members, whether to seek consensus or use a voting process to make decisions. The Project Development Work Group follows the decision-making procedures outlined in the CHORDS Governance Policies and Guidelines.

Meetings
The Project Development Work Group meets monthly. The chairpersons can convene a meeting in the intervening weeks if necessary to discuss time-sensitive opportunities. This charter will be reviewed as needed.

Data Work Group Charter

Overview
The Colorado Health Observation Regional Data Service (CHORDS) is a regional collaborative partnership among Colorado health care delivery systems, public health departments, the Colorado Regional Health Information Organization (CORHIO), and the University of Colorado Anschutz Medical Campus to share health data. CHORDS collects, analyzes and presents data from participating partners' electronic health records (EHRs) to monitor population health, target areas for intervention, and conduct research and evaluation activities. This charter will be reviewed as needed.

Purpose
The Data Work Group is responsible for identifying requirements and standards for data curation, exchange and use.

The Data Work Group oversees the process for defining the data model, proposing modifications including new tables and variables or changes to existing ones and scheduling their implementation on an annual basis. The group is also responsible for implementing a master patient identifier solution.

The Data Work Group provides the Governance Committee with analyses of the benefits and costs of proposed modifications. This group also works closely with the Project Development Work Group to determine the feasibility and costs associated with new requests and adapters.

The Data Work Group is responsible for activities related to data definition and harmonization, and data quality assurance. These activities may require handling of confidential data not for public release.

The Data Work Group may convene Communities of Practice among data partners around specific data-related needs.

Membership
The Data Work Group includes data partners and technology partners. Membership is voluntary.

The Work Group will have two chairpersons, with at least one chairperson also serving as a CHORDS Governing Board member. The chairpersons will serve as liaisons between the Governing Board and the Data Work Group.

Guiding Principles
The Data Work Group follows the principles outlined in the CHORDS Governance Policies and Guidelines.

Decision-making
Consensus-based decisions are preferred; however, decision-making processes will vary depending upon the issue. The Data Work Group chairpersons will determine, with input from the members, whether to seek consensus or use a voting process to make decisions.

The Data Work Group follows the decision-making procedures outlined in the CHORDS Governance Policies and Guidelines.

Meetings
The Data Work Group meets monthly and communicates using email as needed. The chairpersons can convene a meeting in the intervening weeks if necessary to discuss time-sensitive opportunities.

Research Council Charter

Overview
The Colorado Health Observation Regional Data Service (CHORDS) is a regional collaborative partnership among Colorado health care delivery systems, public health departments, the Colorado Regional Health Information Organization (CORHIO), and the University of Colorado Anschutz Medical Campus to share health data. CHORDS collects, analyzes and presents data from participating partners' electronic health records (EHRs) to monitor population health, target areas for intervention, and conduct research and evaluation activities.

Purpose
The Research Council is responsible for fostering high-quality research projects that use and disseminate CHORDS data in analyses. This includes refining research questions with investigators, recommending appropriate and feasible research projects, and assisting the Project Development Work Group and the Governance Committee in prioritizing requests.

The Research Council reviews new research projects; advises potential users of the system, the data available, and necessary IRB and data agreement processes; and manages project planning and timelines for research projects. The Council works with existing data users and engages new users.

Membership
The Research Council includes data partners, data users, technology partners, the researcher leading a given project, and interested stakeholders. Membership in the Council is voluntary. The Council will have two chairpersons, with one chairperson also serving as the Project Manager for Research (PMR). The chairpersons will serve as liaisons between the Research Council, the Governance Committee, the Data Work Group and the Project Development Work Group as needed.

Guiding Principles
The Research Council follows the principles outlined in the CHORDS Governance Policies and Guidelines.

Decision-making
Consensus-based decisions are preferred; however, decision-making processes will vary depending upon the issue. The Research Council chairpersons will determine, with input from the members, whether to seek consensus or use a voting process to make decisions.

The Research Council follows the decision-making procedures outlined in the CHORDS Governance Policies and Guidelines. Final decisionmaking power regarding approval of research requests resides with the Governance Committee. Only aggregate/count PTR requests using the existing data model can proceed with Council approval alone.

Meetings
The Research Council meets monthly. The chairpersons can convene a meeting in the intervening weeks if necessary to discuss time-sensitive opportunities. Communication regarding new projects may also occur over email if needed.

This charter will be reviewed as needed.

Appendix E.: CHORDS Roles and Settings

Definitions:

- Patient-level data: Data in which each row represents one patient's information. May also use terms: record-level, individual-level data.
- Summary data: Data in which counts of the patient records meeting given criteria are returned. May also use term: counts.
- Aggregate data: Data in which results are pooled/consolidated across multiple sites before being returned to investigators and analyzed.
- Site-specific data: Data in which results come from only one site.

Roles and Settings for Data Exchange:

Role	Description	Type of Agreement Governing Role
DataMart Client Administrator (At each data partner site.)	Review and respond to requests via the DataMart Client (both incoming requests and outgoing results).	DUA
	DataMart Administrators may also manage the metadata for their DataMart(s) and submit requests to their own DataMart(s).	
	Regular data uploads and data quality checks. Ensure timing of data updates does not interfere with query submissions and returns.	
Investigator (Data user)	May submit requests and review/export aggregated (not site-specific) results within a Project. Investigators cannot select specific DataMarts; they can set geographic/demographic selection criteria.	DUA
Enhanced Investigator (Data user)	May submit requests and review/export site-specific results for all requests within a Project.	DUA that allows site-specific data sharing. Additional user agreements as required by site.
Network Administrator (UCD)	Manage the network, including creating network entities, managing access controls, and approving or creating users.	
	Submit requests and review results to ensure operations and functionality. Assist investigators and enhanced investigators.	Must be listed on project IRBs/protocols

Appendix F. CHORDS Identity Management

The CHORDS Network is originating a two-step process that securely removes duplicate individuals from distributed queries' prevalence estimates while maintaining its commitment to exchanging the minimum data necessary.

Why care about identity management in the CHORDS Network?

- Health care delivery and payment systems are fragmented.
- Patients increasingly seek care in multiple systems due to specialty referrals, job turnover, and insurance changes.

What principles guide this process?

- CHORDS exchanges the minimum data necessary.
- CHORDS operates with a federated, distributed model.

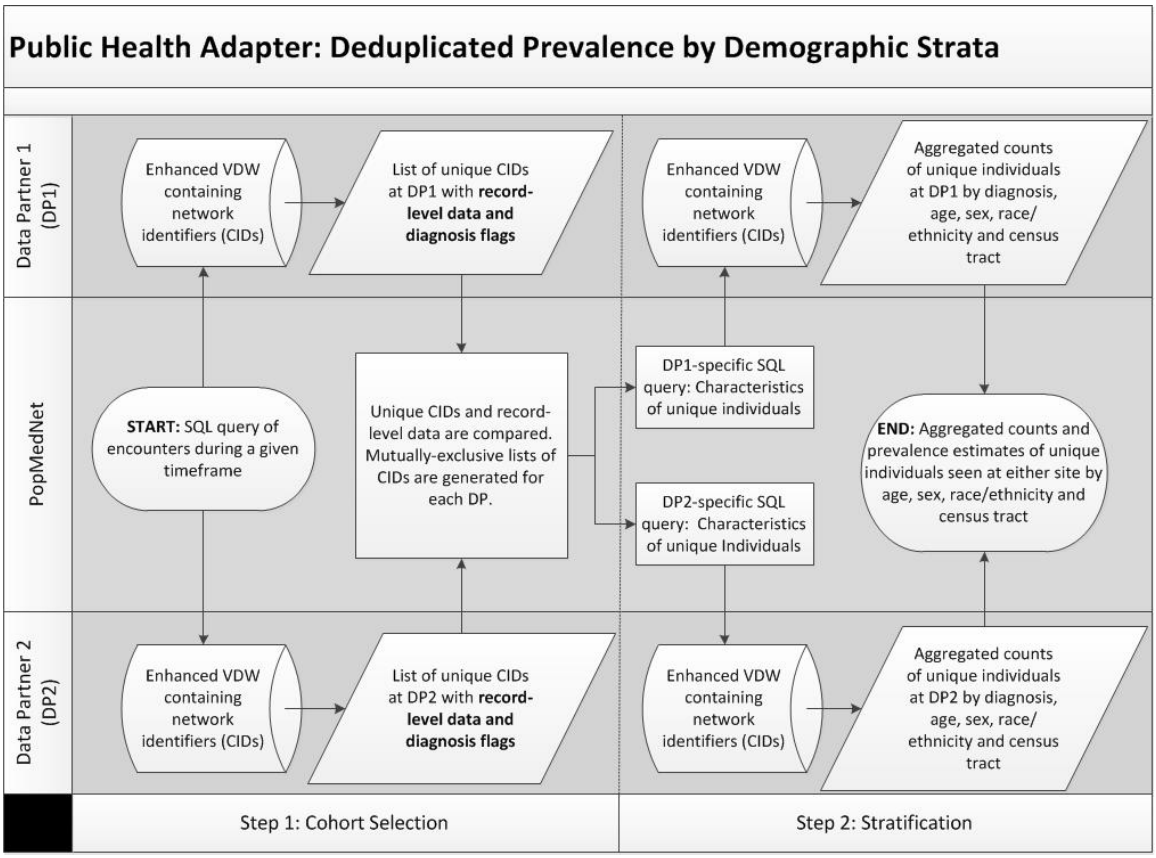
"Step Zero": Setting the Stage

- Relevant infrastructure needs to be in place before prevalence estimates can be deduplicated.
- Data partners have updated their virtual data warehouses to create a table that will store identifiers.
- Data partners work with CORHIO to assign identifiers to their patients by exchanging record-level data outside the CHORDS Infrastructure through a secure FTP site.

Definitions:

- ***Record linkage*:** Identifying an individual who appears in multiple VDWs
- ***Deduplication*:** Using the record linkage process to ensure individuals are only counted once in a population estimate
- ***Identity management*:** All of the tasks and processes that make record linkage and deduplication possible
- ***PERSON_ID*:** An ID specific to a data partner's VDW
- ***CID*:** An ID assigned by CORHIO specific to the CHORDS network. This is not protected health information (PHI).

What is the CHORDS Two-Step Process?



Selecting Individuals for a Site-Specific Query:

1. If a patient is diagnosed at site 1, but not site 2, site 1 contributes data
2. If a patient is diagnosed (or not) at both sites, the site with the most recent visit contributes data
3. If a patient is diagnosed (or not) at both sites, and has identical recent visit dates, the site is randomly selected

Appendix G. CHORDS Data Incident and Response Plan

A **data incident** is a situation in which CHORDS data are released, shared, and/or accessed in a way that is inconsistent with processes approved by COMIRB/IRB of record or executed data use agreements.

Should a data incident occur, this Response Plan will be followed along with appropriate mitigative actions to address the incident. All CHORDS data partners will be notified, within one business day, by the CHORDS board chairperson if a data incident occurs so they can follow their local sites' policies and procedures for reporting and mitigation, if required. A data incident may occur at a data partner site, data user site, CORHIO, or the University of Colorado's Anschutz Medical Campus (CU Anschutz).

Depending on the severity of the data incident (as determined by the Executive Committee in consultation with the CORHIO or CU Anschutz Privacy Officer or others as required), procedures implemented can range from communication/education in the case of a low risk incident; up to contacting CHORDS Network staff to shut down the CHORDS instance of PopMedNet™ in the case of a request that was submitted through PopMedNet™ and resulted in a very high-risk incident.

For data incidents occurring at a data partner site:
a. A DataMart Administrator is responsible for executing all CHORDS queries. Queries will be sent through PopMedNet™ (PMN). Administrators have accountability for returning the query results to the the PMN client. If a data incident occurs at a participating site, the Data Mart Administrator will follow all applicable local policies and procedures for reporting and mitigation of the data incident (i.e., notifying their institution's Privacy Officer, local IRB, and other institutional officials as appropriate). The Data Mart Administrator will also contact the CHORDS Network Administrator as soon as possible or within one business day of the incident occurring.

For data incidents occurring at a data user site:
b. After notifying their local IRB, privacy officer or others as required, the data user will, within one business day, notify the chair of the CHORDS Network Operations Work Group of the data incident issue and the Executive Committee of any mitigative actions taken at their institution including the final resolution of the data incident. The Executive Committee will be responsible for reporting the data incident with all relevant information and within one business day to data partners and COMIRB.

CHORDS also adheres to the following security guidelines of CORHIO (https://www.corhio.org/library/documents/PDF_Collateral/HIE_Privacy_and_Security_Controls.pdf) and the University of Colorado Anschutz Medical Campus (https://www.cu.edu/ois/system-wide-incident-response-procedure-data-breaches) regarding data incidents.

Security

- 9.1 Security Incidents

CHORDS will adhere to CORHIO and CU Anschutz existing policies regarding security incidents and as outlined in this Chapter.

- 9.2 Auditing

Audit Control and Review Plan:

1. Systems and applications to be logged: CHORDS activity is logged for the central portal (web application) hosted at CORHIO on a cloud-based server.
2. Information logged in each system: All data requests submitted through the CHORDS Network are fully logged.
3. Activity reports for each system: CHORDS logs are accessible to CU Anschutz' server network administrators. CHORDS staff request these logs and review them on a quarterly schedule; logs are also available upon request.
4. Procedures to review all audit logs and activity reports, including workforce member responsible for performing the audit, the frequency the audit is to be performed, and escalation procedures if suspicious activity is detected: CHORDS Network Administrators are responsible for regular audits of available logs and activity reports. These audits will be performed quarterly and following any security incidents. If suspicious activity is detected, staff members will report the activity to CHORDS Network Administrators who will report the activity to the University's OIT and adhere to University Incidence Report policies as described in this Chapter's Section 9.3.C.

Audit Trail and Audit Trail Mechanisms

1. Logs contain the information outlined in Chapter 9.2, including user login, login date/time, and activity time.

Workforce Accountability

1. Users are trained on HIPAA accountability through university mandated HIPAA training. Additionally, users agree to adhere to CHORDS and university policies when submitting user access request forms. The policies are located and/or referenced on each form and serve as documentation that staff are trained on these policies.

- 9.4 Workforce Security
  1. Access to Electronic Protected Health Information (ePHI): All individuals accessing ePHI through CHORDS will have the appropriate permission through their project to access ePHI. Each site contributing data to CHORDS must have a DUA in place (or other agreement as required by the institution); each project requesting data from CHORDS must receive IRB approval or exemption and acquire any necessary DUAs from sites (or other agreement as required by the institutions). All individuals accessing CHORDS will be confirmed by their supervisor and by CHORDS administrators as being authorized members of an approved project before being granted access.

     Individuals shall only be granted access to the minimum necessary ePHI that they require to perform their duties.

     All individuals will complete a CHORDS access request form (see Appendix 3). CHORDS adheres to all University policies regarding granting, modifying, and terminating access. Supervisors of approved CHORDS projects will inform CHORDS administrators of any changes in staffing. Individuals no longer associated with an approved project will have their account disabled within one week of termination. In addition, CHORDS requires password changes on a regular basis (6 months); individuals who lose their access to their institutional email account will be unable to change their password and will therefore be locked out of their CHORDS account.

2. Workstation Use and Security
   Individuals accessing ePHI through CHORDS agree to adhere to all policies regarding workstation use and security. CHORDS requires strong passwords and unique user names. Individuals agree to ensure that their workstation settings for all computers used to access ePHI through CHORDS adhere to OIT policy (including regular security patches, standard anti-virus product use, using workstations located in areas with controlled access, etc.). Users agree to use recommended security practices where possible, including encrypting computers used to connect to CUPID; and physically securing computers by working in access-controlled or locked areas and using automatic screen-saver time outs.

- 9.5 Facility and Device Security

Data is stored in New Cloud Data Center, 160 Inverness Dr W #100, Englewood, CO 80112.
Access to the office requires that a NewCloud Employee allows you entrance. Once in the office, physical access to the CORHIO Rack is through an authorized permission list controlled by CORHIO Infrastructure department. The Rack is locked and the key is controlled by NewCloud.

Information is stored on virtual servers running Windows Server 2012. Application runs on the app servers running Microsoft IIS, and the data is stored on the SQL servers running SQL Server 2012. Access is granted to the CHORDS Administrators at CORHIO and UCH

University data is stored in a SQL server and files in the file server at New Cloud Networks/CORHIO. The servers sit behind the New Cloud Firewall and a CORHIO Firewall with New Cloud and CORHIO's security protections.

Backup of the system is preformed through VEEAM Backup and data is retained for 2 weeks. In case of data loss and the need to restore data, these backups would be used to re-populate CHORDS data. CHORDS data is not used for clinical treatment and therefore loss of access to data would not pose an urgent emergency nor a threat to patient safety or wellbeing.

- 9.6 Transmission Security

1. Transmission Security: CHORDS securely transmits data from client datamarts at each data site to a central portal for access by an approved researcher. Only approved projects will receive data through CHORDS transmission. Human review takes place at each site when each query is received and when data is ready for transmission to the researcher. An individual's access to data is limited to the approved project and the minimum necessary data for that individual's role on the project. CHORDS data is accessed via secure file transfer and remote login protocols. CHORDS data is never transmitted via fax.
2. Transmission Security Measures: All transmissions of ePHI from CHORDS to a recipient outside the CHORDS network (e.g. over the Internet) utilize an encryption mechanism. Files containing ePHI are transferred using a secure file transfer protocol. CHORDS does not send e-Mail messages containing ePHI for transmission outside the CHORDS network. See the Secure E-Mail Transmission policy.
3. Integrity Controls: CHORDS has implemented transmission security measures to ensure that ePHI is not improperly modified during transmission. EPHI integrity is sustained using approved mechanisms in transmission from data partners (checksums, hashing algorithms) and to researchers (checksums and hashing algorithms) whenever available and feasible to protect against unauthorized alteration, tampering, corruption, or falsification of the ePHI.

- 9.7 Contingency Plan
  1. Data Backup and Storage Plan: Data contained within CHORDS is not used for patient treatment and therefore immediate recovery of the data is not required in case of an emergency. SQL server data is backed up every 15 minutes. CORHIO performs a full SQL backup nightly, differential backups every hour, and log backups every 15 minutes. This allows CORHIO to restore to any point in time. Full server backups are performed nightly. CORHIO takes a copy of the VM in a consistent state and then have the ability to restore the entire VM, individual disks, or specific files as needed. Backups are performed from a snapshot of the VM while the VM is running.
  2. Disaster Recovery Plan: CHORDS information is not critical for patient treatment and loss of access for a given period of time would not hinder operations. The physical equipment hosting CHORDS is in the NewCloud Networks Office. CHORDS will adhere to the CORHIO disaster recovery plan and provide assistance for CHORDS project-specific needs in the event of an emergency.
  3. Emergency Mode Operation Plan: CHORDS does not provide critical business operations or functions and therefore this Plan is not necessary.
  4. Testing and Revision Plan: This is not a real-time system and therefore a contingency plan in case of emergency and loss of system access is not necessary. CHORDS users would be able to go several weeks without access to the system without impeding business operations.
  5. Applications and Data Criticality Plan: Does not apply, CHORDS functions as one system.
  6. Emergency Access Controls: Does not apply, CHORDS functions as one system with several administrators who can provide access in case of absence of one administrator.

- 9.8 Data Integrity

  1. Integrity Controls: CHORDS uses several standard integrity controls, including:
     a. Firewalls: University data is stored in a SQL server and web application server. The servers sit within CORHIO rack behind the NewCloud and CORHIO firewall.
     b. Password protection: Strong password requirements, user authentication through access request form.
     c. Multi-Factor- Access to the server, requires MFA.
     d. Anti-virus software: All users adhere to CORHIO policies and update anti-virus software as requested.
     e. Standards for change control, testing, documentation, approval, and rollback: Software is developed on a development system. Deployment packages for versions are created and turned over to the administrators to be run on the test system. They run regression testing before deploying a new version to the production server. Extensive documentation of the software development and additional documentation of this process exists.
  2. Data Authentication Controls:
     a. Database integrity: SQL server data is backed up every 15 minutes. We perform a full SQL backup nightly, differential backup every hour, and log backups every 15 minutes. This allows us to restore to any point in time. Backups are performed from a snapshot of the VM while the VM is running. This data is then stored both on local disks for fast restore as well as offsite for long-term archival and DR. No backup data, or any data for that matter, is stored in the cloud.

b. Message integrity: CHORDS will only transmit ePHI using https connections.
c. Procedure integrity: The CHORDS servers are stored in NewCloud Networks Datacenter. It has redundant cooling and power. The room is monitored by cameras and the door is protected by badge and key. CORHIO Racks are only accessible by authorized personnel.

3. Software Controls: SQL server meets the requirements as defined in this Chapter. CHORDS does not allow for the modification of ePHI. Further, the original ePHI remains at its proprietary source and is not accessed at all through CHORDS. No modifications are possible for the ePHI stored in the EHRs at each source institution. Therefore, no modifications can be made which would impact patient treatment or alter a patient's original record.

- 9.9 Person or Entity Authentication

CHORDS uses unique user logins and passwords (which are encrypted when stored). CHORDS users agree to adhere to all policies outlined in this Chapter. CHORDS administrators will ensure prompt deletion of terminated users as outlined in this Chapter.

- 9.10 Device and Media Controls

All ePHI stored on hardware or electronic media will be destroyed prior to the decommissioning of the hardware or media itself in accordance with the policies and methods outlined in this Chapter. Prior to device or media re-use, all ePHI stored on a device or media will be securely removed. While CHORDS does not currently use hardware or electronic media to store ePHI (as ePHI is not transmitted through our system), once these practices are initiated CHORDS will keep a written inventory of hardware and electronic media used to store ePHI as outlined in this Chapter. All research projects using CHORDS data will need to have additional IRB and DUA documentation of the project's procedures and policies around data storage.

- 9.11 Portable Media Security

All CHORDS users agree to adhere to the policies outlined in this Chapter. ePHI will only be stored on portable media devices when necessary. All devices will have security controls in place in accordance with the University's policies, and only minimum necessary data will be stored. Data will be deleted/wiped and/or the device destroyed when the ePHI storage is no longer necessary.

- 9.12 Secure E-Mail Transmission

No ePHI is currently transmitted over email in the CHORDS system. In the future CHORDS will only transmit ePHI using https connections.

- 9.13 Security of ePHI on Home Computers

Initially, CHORDS users will not be accessing ePHI in the data and reports. When ePHI becomes accessible, all CHORDS users agree to adhere to University policies regarding anti-virus software, security patches, anti-spyware software, firewalls, etc. as outlined in this Chapter when using home computers. Each research project using CHORDS will need

to document their data storage policies and procedures in study-specific IRB documents and Data Use Agreements. Additionally, CHORDS recommends that access from home computers take place only using a VPN connection to the University.

Chapter 10 Report a Breach

- 10.1 HIPAA Privacy Incident Notice
    - CHORDS team members will use the appropriate forms and processes from CORHIO and CU Anschutz to notify relevant parties of potential HIPAA privacy incidents
- 10.2 Complaint Notification Form
    - CHORDS team members will use the appropriate forms and processes from CORHIO and CU Anschutz to notify relevant parties of HIPAA Complaint Notifications.

Appendix H. Memorandum of Understanding Template

Colorado Health Observation Regional Data Service (CHORDS)
Memorandum of Understanding

Purpose

The purpose of this memorandum of understanding (MOU) is to clarify the responsibilities of the recipient of data from the Colorado Health Observation Regional Data Service (CHORDS).

This MOU is between CHORDS and (partner).

Background

The Colorado Health Observation Regional Data Service (CHORDS) is a regional collaborative partnership among Colorado health providers, public health departments, the Colorado Regional Health Information Organization (CORHIO), and the University of Colorado Anschutz Medical Campus to share health data. CHORDS collects, analyzes and presents data from participating partners' electronic health records (EHRs) to monitor population health, target areas for intervention, and conduct research and evaluation activities.

CHORDS uses a distributed data approach in which data partners maintain physical and operational control over their electronic data stored in virtual data warehouses (VDWs). CHORDS will aggregate data across data partners, not revealing the source institution. Individual, record-level data may be provided with the appropriate approvals in place, including approval by participating data partners as well as relevant committees (Executive, Governance, Research Council, etc.).

All approved uses of CHORDS data must adhere to the policies and principles outlined in the current CHORDS Governance Plan available at www.CHORDSNetwork.org.

Data Receipt and Use

To be completed

Data Storage and Security

To be completed

Terms

This MOU shall be effective on the date signed by (partner) and will remain in effect for as long as the user is in possession of CHORDS data or unless amended by mutual agreement the CHORDS Network and (partner).

_____
Name:
Date:

_____
Name:
Date: