Title: Data Governance Policy
Date Created: September 13, 2018
Date Modified: September 30, 2025
Date Approved by CCN Board of Directors: November 11, 2025
Date Approved by CCC/IPA Board of Directors: November 19, 2025
Policy# PS22

Purpose:

To establish the governance of data shared by and with Care Compass Entities Staff, Participants, and vendors. This Policy is supported by additional Care Compass Entities privacy and security policies and procedures.

CCN, the Affiliated Entities, and Participants work together to coordinate services among agencies and providers in the CCN and Affiliated Entities region. Care Compass Entities monitor health outcomes in support of emerging networks for value-based contracting.

Definitions:

837 Billing Data: The format established to meet HIPAA requirements for the electronic submission of healthcare claim information. The claim information includes the following for a single care encounter between patient and provider: i) a description of the patient, ii) the patient's condition for which treatment was provided, iii) the services provided, and iv) the cost of the treatment.

Applicable Privacy and Security Laws: HIPAA, as defined below, and all other applicable federal, state, and local laws and regulations that govern the creation, storage, receipt or transmission of individually identifiable medical records or information.

Business Associate Agreement (BAA): A formal written contract between Care Compass Entities and a covered entity or business associate that requires both parties to comply with specific requirements related to PHI.

Care Compass Entity(ies): An organization(s) that is directly, or indirectly through one or more intermediaries, owned or controlled by, or are under common ownership or control of Care Compass Network (CCN), including Care Compass Collaborative, Inc. and Care Compass Supporting IPA, LLC.

Competitively Sensitive Information: Information that could result in anti-competitive discussions or behaviors, including price, cost, output, customers, and strategic planning information.

Commingled Data: Any data set utilized or generated by Care Compass that maintains fields found originally in data provided by multiple data sources, including Participants, Regional Health Information Organizations (RHIO(s)), Statewide Health Information Network for New York (SHIN-NY), public and private payors, and New York State Department of Health (NYSDOH).

CCN Community Consent: A consent workflow enabling Individuals to provide consent with one signature to allow all Community Consent Partners to access their data, consistent with all Applicable Privacy and Security Laws and CCN's and the Affiliated Entities' policies and procedures.

Community Consent Agreement: A consent form that allows for an Individual to provide authorization for Community Consent Partners to access their data.

Community Consent Partners: Participants that have committed to and are participating with CCN's and/or the Affiliated Entities' Community Consent model.

Confidential Information: Information that has been classified by CCN Management, per Appendix B of the Affiliated Entities' CC12 – Antitrust Compliance Policy.

Data Partner: Participants who contribute data for population health analytics, metric improvement, or care coordination purposes.

Data Use Agreement (DUA) (aka Data Partner Agreement): An executed agreement between a data provider and a data recipient that specifies the terms under which the data can be used.

De-identified information - Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the Health Insurance Technology for Economic Clinical Health Act (HITECH) and any regulations, rules, and guidance issued pursuant to HIPAA and the HITECH Act (collectively "HIPAA").

Individual(s): Person(s) covered by public and private payors cared for in the CCN and Affiliated Entities region and uninsured persons, as applicable.

Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- That identifies the individual; or
- With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Participant: Any organization that has signed an Open Network Participation Agreement, an IPA Performance Network Participation Agreement, and/or an agreement related to a funded program with CCN and/or the Affiliated Entities.

Personal, Identifiable Information (PII): Information that can be assumed to identify the individual person including, but not limited to:

- Names of patient, relatives, and employer.
- Address or address codes, email address, IP address, and Universal Resource Locator (URL).
- Birth date, telephone, and fax numbers.
- Social Security, Health Plan Beneficiary, Certificate, License, and Vehicle numbers.
- Medical Record or account numbers.
- Finger or Voice prints and Photographic or Diagnostic images.

▪

Protected Health Information (PHI): Individually Identifiable Health Information, that is transmitted by or maintained in electronic media, or transmitted or maintained in any other form or medium (with exceptions, as described under 45 CFR §160.103), that relates to a person's physical or mental health, and his/her treatment or payment including, but not limited to:

- Name.
- All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code.
- All elements of dates (except year) for dates related to an individual, including birthdate, admission date, discharge date, date of death, and exact age if 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).
- Telephone numbers.
- Facsimile numbers.
- E-mail addresses.
- Social Security numbers.
- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web Universal Resource Locators (URLs).
- Internet Protocol (IP) addresses.
- Biometric identifiers, including finger and voice prints.
- Full face photographs and any comparable images; and
- Any other unique identifying number, characteristic or code.

Qualified Service Organization (QSO): An organization that provides services to a substance use disorder treatment provider ("SUD Provider"), as defined in Part 2 of federal regulations (42 C.F.R. Part 2), and agrees in a written contract with the SUD provider to abide by the requirements of Part 2 in safeguarding protected SUD information. In accordance with Part 2, such services can include data analytics and population health management.

Sensitive Data: Data that is subject to additional privacy and/or consenting practices, including but not limited to, substance use disorder (SUD) and treatment information, HIV status, Mental Health disorders and treatment information, and reproductive health of minors.

Sensitive Information: Information that relates to CCN's and/or the Affiliated Entities' proprietary or otherwise confidential information or Participant's competitive information included, but not limited to:

- Financial payments to participating organizations.
- Contract details with vendors, insurance payors, or participating organizations.
- Any participating organization's proprietary information that could result in anti-competitive discussions or behaviors (including but not limited to salary data, prices or pricing structure, strategic plans).
- Compliance complaints and/or investigations; and
- Confidential employee information.

Staff: Employees, contractors, agents, consultants, volunteers, and others who act on CCN's and the Affiliated Entities' behalf.

Policy: This Policy addresses data governance and data sharing among Care Compass Entities and their Participants, the uninsured population, and Individuals covered by public and private payors. Where variations exist in the governance and/or data sharing requirements, the distinguishing factor will be specifically identified; in all other circumstances, this Policy applies to an all-payor environment.

This Policy pertains to all Staff, vendors, community health teams, Participants, and any other persons who have access to CCN's and the Affiliated Entities' information systems and will describe how Care Compass Entities establish data partnerships and how data shall be received, stored, used, and shared. This Policy also specifically addresses CCN's and the Affiliated Entities' inclusion, use, and treatment of Sensitive Data or other Sensitive Information.

I. Oversight. The Privacy Officer, Security Officer, CCN Information Technology, Informatics and Data Governance Committee, and CCN Compliance and Audit Committee are responsible for overseeing this Policy to ensure that the data generated and received by Care Compass Entities is appropriately utilized and shared with Participants to support the goals of the region, consistent with all Applicable Privacy and Security Laws and CCN's and the Affiliated Entities' policies and procedures.

II. Data Governance Strategy. Care Compass Entities shall ensure that all CCN and Affiliated Entities data governance strategies and practices comply with all approved CCN and Affiliated Entities privacy and security policies, as well as all Applicable Privacy and Security Laws.

a. Care Compass Entities use the following principles in its data strategy:

i. Establish Data Partnerships with Participants. To analyze data that is timely and actionable, Data Partners may contribute 837 Billing Data, clinical, care plan, and Health Related Social Needs (HRSN) data for Individuals that they serve to CCN's data systems/servers.

ii. Leverage Existing Data Channels. Care Compass Entities will leverage the clinical data managed by the RHIO/SHIN-NY, where possible and necessary. In cases where the relevant information cannot be accessed from the RHIOs/SHIN-NY, Care Compass Entities shall seek to incorporate 837 Billing Data, clinical, care plan, and/or HRSN data feeds from Data Partners' Electronic Health Records (EHR) through a separate interface.

iii. Limit Data Integration Effort Required by Participants. Where possible, Care Compass Entities shall provide support and/or reimbursement to Participants for

their efforts that support CCN's and the Affiliated Entities' data strategies, in accordance with CCN's and the Affiliated Entities' policies and procedures and approved programs.

b. Data Use Agreements (DUA(s)) shall be executed with Data Partners and vendors that outline the purpose for data sharing, the data elements to be shared, and the terms of use for the data.
c. Business Associate Agreements (BAA(s)) shall be executed with organizations in combination with contracts where PHI may be shared.
d. Non-disclosure Agreements (NDA(s)) shall be executed with organizations in combination with contracts where Sensitive Information or Confidential Information may be shared.
e. Care Compass Entities shall utilize the minimum necessary standard of the HIPAA Privacy Rule when requesting data from Data Partners.
f. Care Compass Entities shall utilize the minimum necessary standard of the HIPAA Privacy Rule and role-based access when sharing data with Participants, vendors, Staff or other system users, and other entities for which CCN and/or the Affiliated Entities enter an applicable contractual relationship.
g. Care Compass Entities shall further develop, consistent with this Policy, standard definitions of data elements to be shared and guidelines for exchange among CCN, the Affiliated Entities, and Data Partners.
h. Care Compass Entities utilize the standard definition for data breach and breach notification for data shared among CCN, the Affiliated Entities, and Data Partners documented in CCN's and the Affiliated Entities' Breach Notification Policies.
i. PHI, PII, Confidential Information, and Sensitive Information that is not de-identified, redacted, or aggregated is prohibited from being posted to any publicly accessible information system.
j. Staff responsible for administering a CCN or Affiliated Entities program, service, or project where data elements may be exchanged will consult with the Privacy Officer and the Security Officer during program, service, or project planning and development to seek guidance and approval on the data governance strategies and practices to be adopted.

III. Exchange and Data Sharing Agreements

a. Specify the minimum set of controls on responsibility, procedures, technical standards, and solutions.
b. The exchange and data sharing agreements also specify organization policies including:
c. Classification policy for the sensitivity of the business information.
d. Management responsibilities for controlling and notifying transmission, dispatch, and receipt.
e. Procedures for notifying sender of transmission, dispatch, and receipt.
f. Procedures to ensure traceability and non-repudiation.
g. Minimum technical standards for packaging and transmission.
h. Courier identification standards.
i. Responsibilities and liabilities in the event of information security incidents, such as loss of data.
j. Use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected.

k. Ownership and responsibilities for data protection, copyright, software license compliance and similar considerations.
l. technical standards for recording and reading information and software.
m. Special controls that may be required to protect covered items, including cryptographic keys; and
n. Escrow agreements.

IV. Data Sharing.

a. **PHI.** Care Compass Entities may receive PHI that is not considered Sensitive Data from Participants who have entered a BAA with CCN and/or the Affiliated Entities in the following scenarios:
    i. Data submission, including PHI, in support of payments for CCN's and the Affiliated Entities contracted programs. De-Identified Information or aggregated data may be shared with Participants in support of regional common goals, consistent with the terms of the executed DUAs and other CCN and Affiliated Entities Agreements.
    ii. Data submission, including PHI, in support of required audits and other requirements. This data may be shared with auditors, as required. De-Identified Information or aggregated data may be shared with Participants.
    iii. Data on Individuals covered by public and private payors, including PHI, leveraging the RHIOs'/SHIN-NY's commingled data to populate CCN's data systems/servers. An executed DUA is required between CCN and Data Partners for this data exchange. Unless otherwise specified, this data may be shared with other Participants caring for the Individual or that has received a referral for care coordination, or the CCN data systems/servers without explicit consent from the Individual for metric improvement or population health analytics purposes.
        1. Under New York State regulations and privacy and security policies for the SHIN-NY ("SHIN-NY Rules"), Data Partners participating in the SHIN-NY can enter a BAA or so-called One-to-One Exchange arrangement to share patient information through a RHIO with Care Compass Entities as a business associate, consistent with the RHIO consent provided by Individuals and the SHIN-NY Rules.
        2. PHI on Individuals that have executed a Community Consent Agreement can be shared with Community Consent Partners, inclusive of Sensitive Data, consistent with all Applicable Privacy and Security Laws, the DUA, and CCN's and the Affiliated Entities' policies and procedures.

    iv. Data on Individuals, including PHI and HRSNs, to populate CCN's data systems/servers. An executed DUA is required between CCN and Data Partners for this data exchange. This data, except for SUD information and certain reproductive health information may be shared, without explicit consent, from the Individual, unless as otherwise specified by other programs, laws, or regulations with:
        1. other Participants caring for the Individual or that has received a referral for treatment purposes or care coordination.
        2. the CCN data systems/servers.

b. **Competitively Sensitive Information.** Care Compass Entities shall not request Competitively Sensitive Information from Participants, unless otherwise specified in a written agreement between a Participant and CCN and/or the Affiliated Entities and discourages the sharing of Competitively Sensitive Information between Participants in accordance with Antitrust Laws and regulations and the CCN and Affiliated Entities CC12 – Antitrust Policy. Care Compass Entities shall adhere to the Antitrust Policy regarding the sharing of Competitively Sensitive Information with Participants.
c. **Sensitive Information.** Care Compass Entities shall not share Sensitive Information with Participants or other entities, unless prompted by specific CCN and Affiliated Entities Policies and Procedures or is legally required to do so.
d. **HRSN.** In the absence of specific regulations regarding the sharing of this type of data, Care Compass Entities shall treat HRSN data as HIPAA-governed PHI.
e. **Commingled Data.** Care Compass Entities may commingle data received by Data Partners or other sources into data sets for metric improvement and/or care coordination purposes.
f. **Data to Support Population Health.**
    i. CCN and its Affiliated Entities may provide the following data and analysis generated by using contributed data to (a) Participants that care for the Individuals who are the data subjects, and (b) Participants that have contracted with CCN and/or the Affiliated Entities as part of a CCN or Affiliated Entities program to perform care coordination services for the express purpose of improving metrics and/or the health of Individuals.
        1. Lists of high-risk Individuals.
        2. Performance metric dashboards.
        3. Data on gaps in care.
        4. Risk stratification; and
        5. Others need assessments.
    ii. Lists of high-risk Individuals derived from contributed data shall not identify SUD diagnosis or treatment information.

V. Sensitive Data.

a. **SUD Information.** SUD information may be shared with CCN by establishing a direct data transfer between a Data Partner that is an SUD provider and CCN. This data shall not be shared with the Affiliated Entities or other Participants without explicit consent from the Individual, which may include an executed Community Consent Agreement, but may be shared with the CCN data systems/servers. CCN may receive SUD information from Data Partners with the following in place between CCN and the Data Partner:
    i. BAA; and
    ii. DUA that contains the provisions obligating CCN to serve as a QSO.
b. **HIV/AIDS Status.** HIV/AIDS status and related information on Individuals covered by public and private payors may be shared with CCN through the RHIO from Data Partners, who have entered a DUA and BAA with CCN, with explicit consent from the Individual, in accordance with Applicable Privacy and Security Laws. This data may be shared with the CCN data systems/servers but may not be shared with the Affiliated Entities or other Participants caring for the Individual or that has received a referral for care coordination, without explicit consent from the Individual, which may include an executed Community Consent Agreement.

c. **Mental Health Information.** Mental Health diagnosis and treatment information on Individuals covered by public and private payors may be shared with CCN, in accordance with Applicable Privacy and Security Laws, from Data Partners who have entered DUA and BAA with CCN by establishing direct data transfer between the Data Partner and CCN. This data may be shared with the CCN data systems/servers but may not be shared with the Affiliated Entities or other Participants caring for the Individual or that has received a referral for care coordination, without explicit consent from the Individual, which may include an executed Community Consent Agreement.
    i. Information about Mental Health diagnosis and treatment provided by health care providers or facilities that are not licensed by the New York State Office of Mental Health (OMH) or Office for People with Developmental Disabilities (OPWDD), including primary care physicians, psychiatrists, and others, may be received, and used pursuant to HIPAA.

VI. CCN Community Consent. CCN and its Affiliated Entities will coordinate the implementation and management of the CCN Community Consent, utilizing the Community Consent Agreement, to facilitate regional data sharing for collaborative care, population health, and care coordination activities. Where possible, existing consent management tools and processes will be leveraged.

a. The Community Consent Agreement will include, but not be limited to, the following requirements:
    i. Provide Individuals with the option to give or deny consent to all Community Consent Partners, individual Partners, or all Community Consent Partners with exceptions noted.
    ii. Compliance with 42 CFR Part 2 requirements.
    iii. A description of the information to which the patient is granted access, including specific reference to HIV, mental health, substance use disorder, reproductive health, and genetic testing information, with the ability to exclude such information as desired.
    iv. A description of the intended uses such as treatment or care management.
    v. The name of the source(s) of the information.
    vi. A link for the Individual to access the list of all Community Consent Partners, which will be updated online within 24 hours of a change and will be available by mail upon request within 5 days of notice of request; and
    vii. A digital or written signature of the Individual or an authorized representative.
b. Community Consent Partners will abide by the following requirements to participate in CCN Community Consent:
    i. Utilize the Community Consent Agreement designated by Care Compass Entities.
    ii. Follow the procedures developed for consent management, such as updating consent management tools with Individual information and executed Community Consent Agreements; and
    iii. Maintain compliance with applicable Minimum Necessary Rule requirements under the HIPAA Privacy Rule and/or other Applicable Privacy and Security Laws.

VII. Termination of Data Partnership and Data Destruction. Upon termination of the Data Partnership, Care Compass Entities shall delete the applicable data contributed by the Data Partner, if feasible, consistent with Applicable Privacy and Security Laws and applicable medical protocols. When data is required to be deleted in this scenario, Care Compass Entities shall require

system vendors to extract and delete pertinent Data Partner data in commingled data sets and shall receive certification of data destruction from the applicable vendors. If data destruction is not feasible, Care Compass Entities shall provide written certification that all pertinent Data Partner data not destroyed shall be protected as provided in this Policy. CCN shall include in all DUAs the right for Data Partners to terminate data partnership at any time for any reason.

CCN Board Approval History: 11/13/2018, 10/8/2019, 12/8/2020, 1/11/2022, 10/8/2024, 11/11/2025

CCC/IPA Board Approval History: 11/12/2024, 11/19/2025

Compliance and Audit Committee Review History: 7/16/2019, 6/30/2020, 8/30/2021, 11/2/2022, 3/28/2024, 5/22/2024

IT & Data Governance Committee Review History: 7/17/2024, 11/10/2025

Policy Revisions:

Date	Revision Log	Updated By
9/13/2018	Original creation	Rebecca Kennis
7/16/2019	(1) Edits to allow for data sharing of Medicaid member data utilizing the Medicaid application as consent; (2) CCN requirement to protect data not destroyed due to infeasibility post termination of Data Partnership; (3) Clarification of the scope of data types and sources covered under this policy; (4) Language added to require contractual rights to assign system contracts to a designated organization; (5) System decommission requirements	Rebecca Kennis
6/30/2020	(1) New definitions added for Community Consent, Community Consent Agreement, and Community Consent Partners; (2) New phrases to include Community Consent as a recognized form of explicit patient consent, where explicit consent is required, inclusive of SUD; (3) A new section was added outlining the guidelines and requirements for Community Consent.	Rebecca Kennis
8/30/2021	(1) Language updated to remove references and data sharing permissions/restrictions associated with DSRIP and MCD, with the exception for a reference to data sharing with NYSDOH in the instance of a DSRIP audit; (2) Added to Data Governance Strategy requirements for DUAs, BAAs, NDAs, minimum necessary standard, and data protection on publicly-accessible systems; (3) Moved Assignability and System Decommission language to PS18 – Systems and Services Acquisition Policy; (4) Removed restriction of CCN's data focus being only Medicaid and the uninsured populations to allow for potential future opportunities.	Rebecca Kennis
11/2/2022	(1) Throughout the policy, acronyms and initialisms were amended to spell out the full name of the organization on first reference (e.g., RHIO, NYSDOH, DSRIP); (2) Added defined term for Data Use	Rebecca Kennis

	Agreement (DUA), using NIST definition; (3) Clarified definition of Partner Organization to reflect participation in the Open Network; (4) Removed the word "clinical" from the data strategy principle of "Leveraging Existing Clinical Data Channels" to match the text in that section as not being limited to clinical data.	
6/24/2024	Updated to an enterprise-wide policy; updated Section II(j) to include the requirement for guidance and approval on data governance strategies from the Privacy and Security Officers during program development; removed DSRIP audit requirement; replaced "Medicaid" throughout to allow for data governance on potential programs with other payors;	D. Hodges, K. Green A. Rotella
9/30/2025	Added definitions for Individually Identifiable Health Information, Care Compass Entity(ies) and updated definition of PHI. Added Exchange and Data Sharing Agreements section. Updated Affiliated Entities to Care Compass Entities	Dustin Moore Kim Loveless C Petrak

This Policy shall be reviewed periodically, but no less than once every 12 months, and updated consistently with the requirements established by the Board of Directors, Care Compass Network's Leadership Team, Federal and State law(s) and regulations, and applicable accrediting and review organizations.