Title: Privacy Program Policy
Date Created: April 4, 2022
Date Modified: May 9, 2025
Date Approved by CCN Board of Directors: June 10, 2025
Date Approved by CCC Board of Directors: January 28, 2025
Date Approved by IPA Board of Directors: September 24, 2024
Policy # PS24

Purpose:

This policy serves to establish the privacy requirements for the Care Compass Entities and Affected Individuals and Business Associates consistent with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule.

Definitions:

Affected Individual(s): All persons who are affected by Care Compass Entities' risk areas including Care Compass Entities' employees, officers, Directors, managers, contractors, agents, subcontractors, independent contractors, governing bodies, or third-parties, who or that, in acting on behalf of the Care Compass Entities: (i) delivers, furnishes, directs, orders, authorizes, or otherwise provides health or social care items and services under State, Federal, or Care Compass programs; and (ii) contributes to the Care Compass Entities' entitlement to payment under Federal health or social care programs, or from other payor sources.

Business Associate: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

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

Care Compass Entities: Organizations that are directly, or indirectly through one or more intermediaries, owned or controlled by, or are under common ownership or control of, Care Compass Network, including Care Compass Collaborative, Inc. ("CCC") and Care Compass Supporting IPA, LLC ("IPA").

Covered Entity: A health plan, healthcare provider, or healthcare clearinghouse that must comply with the HIPAA Privacy Rule.

Disclose(s)/Disclosure(s): For information that is protected health information, disclose or disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the Care Compass Entities with a business need to know.

Health Care Operations: Any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities,

including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of a Covered Entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of a Covered Entity.

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").

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

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. 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
    a. That identifies the individual; or
    b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Loco parentis: "In place of a parent", refers to the legal responsibility of a person or organization to take on some of the functions and responsibilities of a parent.

Participant: Any organization that has signed an agreement related to a funded program with the Care Compass Entities.

Payment: Activities to obtain premiums, to determine or to fulfill responsibilities for coverage and provision of benefits, or to furnish or receive payment for health care delivered to an individual, or to a group, and activities of a health care provider to obtain payment or to be reimbursed for the provision of health care to an individual, or to a group, including but not limited to value based arrangements.

Personal Identifiable Information ("PII"): Information that can be reasonably 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.

Personal Representative(s): A person authorized (under State or other applicable law, e.g., tribal or miliary law) to act on behalf of an individual in making care related decisions.

Privacy Rule: The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996. The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") standards address the use and disclosure of individuals' health information ("PHI") by organizations subject to the Privacy Rule, Covered Entities, as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule.

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:

1. Name;
2. 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;
3. 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);
4. Telephone numbers;
5. Facsimile numbers;
6. E-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) addresses;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographs and any comparable images; and
18. Any other unique identifying number, characteristic or code.

Sensitive Information: Information that relates to the Care Compass Entities' proprietary information or a participating organization's competitive information including, but not limited to:

- Financial payments to participating organizations;
- Contract details with vendors, 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);
- Organizational compliance complaints and/or investigations;

- Sensitive 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; and
- Confidential employee information.

Staff: Employees, contractors, agents, consultants, volunteers, and others who act on the Care Compass Entities' behalf.

Treatment: The provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.

Use(s): The sharing, employment, application, utilization, examination, or analysis of PHI, PII, and/or Sensitive Information by any person working for or within the Care Compass Entities, or by a Business Associate of the Care Compass Entities.

Policy:

It is the policy of the Care Compass Entities to implement measures and controls to protect the privacy and confidentiality of PHI, PII, and Sensitive Information. The Care Compass Entities are dedicated to the protection of information pertaining to its Affected Individuals and the patients and clients served by its Affected Individuals.

I. Oversight. The Director of Compliance is responsible for ensuring that privacy measures are assessed, developed, implemented, and maintained to protect the confidentiality, integrity, and availability of PHI, PII, and Sensitive Information under the guidance and oversight of the applicable Compliance Committee(s).

II. Business Associate Agreements ("BAA"). The Care Compass Entities will enter into BAAs with Covered Entities, Business Associates, subcontractors, vendors, Members, Participants, and any other Affected Individuals who have access to PHI under a service agreement to ensure that PHI is appropriately safeguarded by all parties. Any such BAA must:

a. Establish the permitted and required Uses and Disclosures of PHI by the Business Associate;
b. Provide that the Business Associate will not Use or further Disclose the PHI other than as permitted or required by the BAA or as required by law;
c. Require the Business Associate to implement appropriate safeguards to prevent unauthorized Use or Disclosure of the PHI, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI;
d. Require the Business Associate to report to the Covered Entity any Use or Disclosure of the PHI not provided for by its service agreement and BAA, including incidents that constitute breaches of unsecured PHI;
e. Require the Business Associate to document Disclosures of PHI, as specified in its BAA, and make accountings of Disclosures available to Covered Entity upon request;
f. To the extent the Business Associate is to carry out a Covered Entity's obligation under the Privacy Rule, require the Business Associate to comply with the requirements applicable to the obligation;

g. Require the Business Associate to make available to HHS its internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received by the Business Associate on behalf of the Covered Entity for purposes of HHS determining the Covered Entity's compliance with the HIPAA Privacy Rule;
h. At termination of the service agreement and BAA, if feasible, require the Business Associate to return or destroy all PHI received from, or created or received by the Business Associate on behalf of the Covered Entity;
i. Require the Business Associate to ensure that any subcontractor it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the Business Associate with respect to such PHI; and
j. Authorize termination of the BAA by the Covered Entity if the Business Associate violates a material term of the BAA.

III. Access to PHI - Notice of Privacy Practices.

a. The Care Compass Entities will grant access to PHI based on Affected Individuals job functions and responsibilities.
    i. The Director of Compliance, serving as the Privacy Officer, in collaboration with the IT Security Officer, is responsible for the determination of which Affected Individuals require access to PHI and what level of access they require.
    ii. In accordance with HIPAA and State criteria relating to Participants and Business Associates, CCC shall include access to PHI with regard to Business Associates and Covered Entities providing services pursuant to approved Managed Care Organization requirements, which will adhere to all Privacy and Security Policies of Care Compass Entities, and will include the provision of the current Notice of Privacy Practices to recipients served by CCC, its Business Associates, and Participants.
b. In instances where Care Compass Entities are functioning as a Business Associate, the Care Compass Entities will:
    i. Make available to a Covered Entity, information necessary for Covered Entity to give individuals their rights of access, amendment, and accounting of Disclosures in accordance with HIPAA regulations.
    ii. Upon request, make internal practices, books, and records, including policies and procedures, relating to the Use and Disclosure of PHI received from, or created or received by the Compass Care Entities on behalf of a Covered Entity available to the Covered Entity or the Secretary of the HHS for the purpose of determining compliance with the terms of the BAA and HIPAA regulations.
c. In instances where CCC is functioning as a Covered Entity, CCC is required to provide access to PHI:
    i. To individuals (or their Personal Representatives) specifically when they request access to, or an accounting of disclosures of, their PHI; and
    ii. To HHS when it is undertaking a compliance investigation or review or enforcement action.

IV. Use and Disclosure of PHI. The Care Compass Entities will Use and Disclose PHI only as permitted under HIPAA.

a. In instances where the Care Compass Entities are functioning as Business Associates, the Care Compass Entities may:
    i. Use PHI for management, administration, data aggregation, and legal obligations to the extent such Use of PHI is permitted or required by a BAA and not prohibited by law;
    ii. Use or Disclose PHI on behalf of, or to provide services to, Covered Entities for purposes of fulfilling its obligations under a service agreement to them, if such Use or Disclosure of PHI is permitted or required by the BAA and would not violate the HIPAA Privacy Rule; or
    iii. In the event that PHI must be Disclosed to a subcontractor or agent, the Care Compass Entities will enter into a BAA with the subcontractor or agent that ensures the subcontractor or agent agrees to abide by the same restrictions and conditions that apply to the Care Compass Entities under the BAA with respect to PHI, including the implementation of reasonable and appropriate safeguards.

b. In instances where CCC is functioning as a Covered Entity;
    i. Required Disclosures. CCC must Disclose PHI:
        1. To individuals (or their Personal Representatives) specifically when they request access to, or an accounting of disclosures of, their PHI; and
        2. To HHS when it is undertaking a compliance investigation or review or enforcement action.
    ii. Permitted Uses and Disclosures. CCC may, but is not required, to Use and Disclose PHI, without an individual's authorization, for the following purposes or situations:
        1. To the individual (unless required for access or accounting of disclosures);
        2. For its own Treatment, Payment, and Health Care Operations activities, or for the Treatment activities of any health care provider, the Payment activities of another Covered Entity and of any health care provider, or the Health Care Operations of another Covered Entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both Covered Entities have or had a relationship with the individual and the PHI pertains to the relationship;
        3. With opportunity to agree or object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object;
        4. Incident to an otherwise permitted Use and Disclosure;
        5. For public interest and benefit activities, such as:
            a. When required by law;
            b. Public health activities;
            c. In certain circumstances to appropriate government authorities regarding victims of abuse, neglect, or domestic violence;
            d. Health oversight agency legally authorized activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs;
            e. In a judicial or administrative proceeding through an order from a court or administrative tribunal or in response to a subpoena or other lawful process;

f. To law enforcement officials for law enforcement purposes;
g. To funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law;
h. To facilitate the donation and transplantation of cadaveric organs, eyes, and tissue;
i. For research purposes, without an individual's authorization, provided CCC obtains either:
    i. documentation that an alteration or waiver of individuals' authorization for the Use or Disclosure of PHI about them for research purposes has been approved by an Institutional Review Board or Privacy Board;
    ii. representations from the researcher that the Use or Disclosure of the PHI is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any PHI from the Care Compass Entities, and that PHI for which access is sought is necessary for the research; or
    iii. representations from the researcher that the Use or Disclosure sought is solely for research on the PHI of decedents, that the PHI sought is necessary for the research, and, at the request of the Care Compass Entities, documentation of the death of the individuals about whom information is sought. The Care Compass Entities may also Use or Disclose, without an individual's authorization, a limited data set of PHI for research purposes;
j. When CCC believes it is necessary to prevent or lessen a serious and imminent threat to a person or the public or to law enforcement to identify or apprehend an escapee or violent criminal;
k. For certain essential government functions; and
l. As authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

6. The Use or Disclosure of a limited data set, or PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed, for research, Health Care Operations, and public health purposes, provided the recipient has entered into a data use agreement with CCC which specifies the safeguards for the PHI within the limited data set.

c. Scope of Disclosure: Minimum Necessary Standard.
    i. Affected Individuals with access may Use and Disclose PHI as required under HIPAA, but the PHI Disclosed must be limited to the minimum amount necessary to accomplish the purpose of the Use, Disclosure, or request.
d. The Care Compass Entities may use PHI to report violations of law to appropriate federal and state authorities.

V. **Privacy Safeguards.** The Care Compass Entities have implemented appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of PHI, PII, and Sensitive Information. Such safeguards:

a. Require that the Care Compass Entities acquire and use PHI, PII, or Sensitive Information obtained only as necessary to perform its services and support functions related to the health and health related social needs of the community;
b. Limit access of such information to those Affected Individuals who perform identified service and support functions;
c. Prohibit Disclosure of PHI, PII, or Sensitive Information to persons who are not Affected Individuals of the Care Compass Entities in the absence of express approval from legal counsel and, if appropriate, the customer and/or patient;
d. Require all Affected Individuals of the Care Compass Entities to report Uses and Disclosures of PHI, PII, or Sensitive Information that are not permitted by this Policy;
e. Require that the Care Compass Entities investigate all reports that PHI, PII, or Sensitive Information was used in a manner not permitted by its Privacy and Security Policies and will impose appropriate sanctions for conduct prohibited by the Privacy and Security Policies;
f. Establish that Affected Individuals receive training upon hire, appointment, or contractual relationship regarding the Care Compass Entities' Privacy and Security Policies and the importance of protecting the privacy of PHI, PII, or Sensitive Information, and annually thereafter; and
g. Provide for the storage and transmission of PHI, PII, or Sensitive Information in a secure manner that protects the integrity, confidentiality and availability of the information.

VI. **Mitigation of Harm.** In the event of a Use or Disclosure of PHI that is in violation of the requirements of a BAA or this Policy, the Care compass Entities will mitigate, to the extent practicable, any harmful effect resulting from the violation.

a. Such mitigation includes:
    i. Reporting any Use or Disclosure of PHI not provided for by the BAA and any privacy incident of which the Care Compass Entities become aware to the Director of Compliance and Covered Entity, as applicable, pursuant to the Care Compass Entities' Breach Notification Policy; and
    ii. Documenting such Disclosures of PHI and information related to such Disclosures as would be required for Covered Entity to respond to a request for an accounting of Disclosure of PHI in accordance with HIPAA.

VII. **Personal Representatives.** In instances where CCC is functioning as a Covered Entity, Personal Representatives may have broad authority to act on behalf of an individual in making decision related to health and/or social care, where relevant to such personal representation.

a. CCC may provide an individual's Personal Representative with:
    i. an accounting of disorders,
    ii. access to the individual's PHI,
    iii. the ability to authorize Disclosures of the individual's PHI,
    iv. the ability to sign consents,
    v. copies of health-related social care records, and

vi. authorization to complete health-related social needs screenings and accept navigation to eligible services.

b. Adults and Emancipated Minors.
    i. A minor is emancipated under the following conditions:
        1. is a parent of a child, in which case he/she may also consent for his/her child;
        2. is married;
        3. is pregnant;
        4. is living apart from and is financially independent from his/her parent(s) or guardian(s);
        5. is a homeless youth; or
        6. receives services at an approved runaway and homeless youth crisis services program or a transition independent living program.
    ii. The following individuals may serve as an adult's or emancipated minor's Personal Representative, upon verification of broad authority to make decisions related to health and/or social care and relevant to such personal representation:
        1. Court appointed legal guardian or guardian ad litem:
        2. Health care power of attorney;
        3. General power of attorney or durable power of attorney that includes the power to make health care decisions.

c. Unemancipated Minors:
    i. For the purposes of health care in New York State, an unemancipated minor is a person who is under 18 years of age.
    ii. Unemancipated minors are not legally qualified to authorize treatment with certain exceptions, therefore, consent must be obtained from the minor's parent, legal guardian, a *loco parentis,* or other legally empowered individual.
    iii. CCC will comply with all legal requirements and obligations relating to the PHI of minors. Under most circumstances, a parent or legal guardian will have legal authority to act on behalf of minor children. If a parent, guardian, or other person acting in *loco parentis* (i.e., foster parent) has broad authority to act on behalf of an unemancipated minor in making decisions related to health care, CCC will treat such a person as a Personal Representative with respect to PHI relevant to such representation.
        1. There are certain circumstances where a minor has authority to make his/her health care decisions; when a minor has the right to under state law and the minor has not requested another person not be treated as their Personal Representative; when a minor has the right to obtain a particular health care service; or when a guardian agrees to an agreement of confidentiality between a health care provider and the minor.

d. Deceased Individuals.
    i. If under applicable law an executor, administrator, or other person has legal authority to act on behalf of a deceased individual, or the individual's estate, CCC must treat such person as a Personal Representative, with respect to PHI relevant to such personal representation.

e. Abuse, Neglect, and Endangerment Situations.

i. CCC need not release PHI to a Personal Representative if there is reasonable belief that:
    1. the individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
    2. releasing the PHI could endanger the individual; or
    3. it is not in the best interest of the individual to treat the person as the individual's Personal Representative, based on the professional judgement of a qualified employee of CCC.

f. CCC Staff will verify proof of a Personal Representative to act on behalf of an individual in accordance with the Personal Representative(s) Procedure.

VIII. Document Retention. Each Care Compass Entity shall maintain the following for a minimum of six (6) years from the date of its creation, or the date when it was last in effect, whichever is later:

a. A written or electronic record of a designation of the organization as a Business Associate or a Covered Entity;
b. Policies and Procedures implemented to comply with HIPAA;
c. All documented assessments required by HIPAA;
d. All signed Authorization for Release of Health Information Forms;
e. The Notice of Privacy Practices;
f. Documentation of the titles of the persons or offices responsible for HIPAA compliance;
g. Documentation related to HIPAA privacy complaints by a client or patient of a Member;
h. Documentation of HIPAA education provided; and
i. Accounting of disclosures of PHI.

IX. Sanctions. Staff who fail to comply with the privacy policies and procedures of the Care Compass Entities will be subject to disciplinary action, up to and including termination of employment. The Care Compass Entities will ensure that sanctions are applied consistently and fairly to Affected Individuals who fail to comply with the privacy policies and procedures of the Care Compass Entities, according to the Sanctions Policy.

X. Review and Revision. The privacy requirements in this Policy will be reviewed by the Director of Compliance at least annually, when information protection requirements change, when incidents occur, or a substantive change in the Care Compass Entities environment or operations that may impact privacy occurs for consistency with industry best practices and standards and the Care Compass Entities' policies and procedures.

XI. Notice of Privacy Program Policy. The Director of Compliance is responsible for publicizing the Privacy Program Policy, at least annually, in the Care Compass Entities common areas, shared file locations, and on its website for access by Affected Individuals.

CCN Board Approval History: 6/14/2022, 11/08/2022, 8/08/2023, 8/13/2024, 2/11/2025, 6/10/2025

CCC Board Approval History: 9/12/2023, 9/24/2024, 1/28/2025

IPA Board Approval History: 9/12/2023, 9/24/2024

Compliance Committee Review History: 5/13/2022, 11/1/2022, 7/28/2023, 7/24/2024, 1/22/2025, 5/22/2025

Policy Revisions:

Date	Revision Log	Updated By
4/4/2022	Original creation	Cathy Petrak
11/2/2022	Updated list of identifiers in PHI definition, added sensitive data to Sensitive Information definition	Cathy Petrak
7/14/2023	Added Participant definition and Director of Compliance title throughout	Cathy Petrak
8/6/2024	Updated to an enterprise-wide policy; updated to include Privacy Program requirements when CCN and/or its Affiliated Entities are functioning as a covered entity under HIPAA	Cathy Petrak
1/10/2025	Updated Section III to include provision of Notice of Privacy Practices to recipients served by CCC; added Section VIII to include application of sanctions for non-compliance with privacy policies and procedures	Bond, Schoeneck & King
5/9/2025	Added Personal Representative definition and section VII in instances when CCC is functioning as a covered entity; Updated "Affiliated Entities" to "Care Compass Entities" throughout. added "Affected Individuals" definition and updates where applicable	C. Petrak

This Policy shall be reviewed periodically, but not less than once every 12 months, and updated consistent 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.