Title: Privacy Program Policy
Date Created: April 4, 2022
Date Modified: July 14, 2023
Date Approved by Board of Directors: August 8, 2023
Policy # PS24

Purpose:

This policy serves to establish the privacy requirements for Care Compass Network's ("CCN") Staff, vendors, and Business Associates.

Definitions:

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 Care Compass Network and a covered entity that requires both parties to comply with specific requirements related to PHI.

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 Care Compass Network with a business need to know.

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").

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

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.

Protected Health Information (PHI): Information 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 CCN's 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 CCN's behalf.

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

Policy:

It is the policy of CCN to implement measures and controls to protect the privacy and confidentiality of PHI, PII, or Sensitive Information. CCN is dedicated to the protection of information pertaining to its Staff, Business Associates, and the patients and clients served by its participating organizations.

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 Compliance and Audit Committee.

II. Business Associate Agreements. CCN will enter into BAAs with Covered Entities, Business Associates, subcontractors, vendors, participating organizations, and any other persons who have access to PHI under a service agreement to ensure that protected health information 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 the Secretary of the U.S. Department of Health and Human Services ("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. CCN will grant access to PHI based on Staff job functions and responsibilities.

a. The Director of Compliance, in collaboration with the IT Security Officer, is responsible for the determination of which individuals require access to PHI and what level of access they require.

b. As provided in a BAA, CCN will 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.
c. Upon request, CCN will 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 CCN 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.

IV. Use and Disclosure of PHI. CCN will Use and Disclose PHI only as permitted under HIPAA.

a. CCN may 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.
b. Scope of Disclosure: Minimum Necessary Standard.
    i. Staff 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.
c. CCN may 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 would not violate the HIPAA Privacy Rule.
d. In the event that PHI must be Disclosed to a subcontractor or agent, CCN 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 CCN under the BAA with respect to PHI, including the implementation of reasonable and appropriate safeguards.
e. CCN may also use PHI to report violations of law to appropriate federal and state authorities.

V. Privacy Safeguards. CCN has implemented safeguards that execute BAA requirements and reasonably and appropriately protects the confidentiality, integrity, and availability of PHI, PII, or Sensitive Information received, maintained, or transmitted on behalf of Business Associates and the patients and clients served by Participants. Such safeguards:

a. Require that CCN acquires and uses PHI, PII, or Sensitive Information obtained only as necessary to perform its services and support functions related to the health and social determinants of health needs of the community;
b. Limit access of such information to those Staff, subcontractors, or agents who perform identified service and support functions;
c. Prohibit Disclosure of PHI, PII, or Sensitive Information to persons who are not Staff, subcontractors, or agents of CCN in the absence of express approval from legal counsel and, if appropriate, the customer and/or patient;
d. Require all Staff, subcontractors, or agents of CCN to report Uses and Disclosures of PHI, PII, or Sensitive Information that are not permitted by this Policy;
e. Require that CCN 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 CCN Staff receive training upon hire regarding CCN's 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, CCN 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 CCN becomes aware to the Director of Compliance and Covered Entity, as applicable, pursuant to the CCN 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. 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 CCN environment or operations that may impact privacy occurs for consistency with industry best practices and standards and CCN's policies and procedures.

VIII. Notice of Privacy Program Policy. The Director of Compliance is responsible for publicizing the Privacy Program Policy, at least annually, in CCN's common areas, shared file locations, and on its website for access by Staff, vendors, community health teams, and participating organizations.

Board Approval History: 6/14/2022, 11/08/2022, 8/08/2023

Committee Review History: 5/13/2022, 11/1/2022, 7/28/2023

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

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.