CareNu		Effective Date:	11/10/2023
Policy Title:	Health Equity Data Privacy Policy	Last Review Date:	11/10/2023
Issuing Department:	Systems	Last Revision Date:	11/10/2023
Policy Number:	HE.02.06	Next Review Date:	11/10/2024
Applies to:	☐ ACO ☐ MSO ☐ TPA ☒ ALL		

Policy

CareNu is committed to protecting the privacy and confidentiality of individual-level data, particularly sensitive information such as race, ethnicity, language, gender identity, and sexual orientation data. This policy outlines the controls for physical and electronic access to data, permissible and impermissible use of data, and procedures for governing and tracking devices and media containing sensitive information.

Purpose

To provide guidance on the protection, privacy and confidentiality of individual-level data related to health equity.

Scope

This process applies across the organization.

Definitions

N/A

Procedure

1. Access Controls:

1.1. Governing and Tracking:

CareNu Information Technology department will govern and track the receipt, removal, and access to devices and media containing individual-level race and ethnicity, language, gender identity, and sexual orientation data. This includes, but is not limited to, diskettes, CDs, tapes, mobile applications, portable drives, laptops, and secure portals.

1.2. Access Limitation:

To minimize the risk of impermissible access, CareNu will limit employee access to sensitive information only to those employees who require it for their job responsibilities. Access will be terminated promptly for employees who are no longer authorized to have such access.

1.3. Data Storage:

Media and devices containing sensitive information must be stored securely, and access controls must be implemented to ensure only authorized personnel can retrieve and utilize the data. If data is printed for any reason, it must be stored in a locked file cabinet and properly disposed of for secure shredding in an appropriate disposal location on-site at CareNu's office building. Protected electronic data must remain on physically secure media and maintained in password-protected data sources (data warehouse) and on password protected devices (including, but not limited to laptop, cellular phone).

1.4. Reuse of Media and Devices:

Media and devices that have contained sensitive information must undergo thorough cleansing processes to ensure complete removal of data before reuse or disposal.

2. Permissible Use of Data:

2.1. Internal Analyses and Reporting:

Sensitive data may be used for internal analyses and reporting to enhance organizational effectiveness.

2.2. Assessing Healthcare Disparities:

Data can be used to assess healthcare disparities and develop strategies for improvement.

2.3. Designing Intervention Programs:

Sensitive information may be utilized in designing intervention programs to address specific healthcare needs.

2.4. Outreach Materials:

Data can be used in the design and direction of outreach materials to improve community engagement.

2.5. Informing Healthcare Practitioners:

Sensitive information may be shared internally to inform healthcare practitioners and providers about individual language and demographic needs.

2.6. Clinical Care:

Data may be accessed and used in the provision of clinical care to individuals.

2.7. Data Sharing with Vendors:

Data may be shared with vendors for data analytics purposes, such as care management platforms or predictive analytics platforms, under strict confidentiality agreements.

3. Impermissible Use of Data:

3.1. Denial of Services or Coverage:

Any use of personal health information for activities leading to denial of services, coverage, or benefits is strictly prohibited.

3.2. Disclosure to Unauthorized Users:

Unauthorized disclosure of sensitive information to individuals or entities not authorized to access such data is strictly prohibited.

3.3. Inappropriate Treatment at the Point of Care:

The use of data to influence how a patient is treated at the point of care is strictly prohibited.

3.4. Misuse with CareNu Employees:

Using sensitive information inappropriately when engaging with CareNu employees is strictly prohibited.

4. Enforcement and Compliance:

Violations of this policy will result in disciplinary action, up to and including termination of employment. CareNu will regularly review and update this policy to ensure its effectiveness and compliance with applicable laws and regulations.

5. Additional Data Compliance:

In addition to this outlined policy, the following policies must be followed regarding privacy and proper use of data:

- Confidentiality of Information

- Electronic Communications Systems, Acceptable Use
- HIPAA Privacy – Access, Authorization, Use and Disclosure of Protected Health Information

References

[Reference any law, regulation or standard that applies to this policy. **For Example**: 42 C.F.R. §§ 422.564 and 423.564]

Approval/Revision History

Version Number	Change Date; (Original/ Reviewed/ Revised)	First Level Approval	Second Level Approval
V1	11/10/2023 Original	Name: Matthew Strohhacker Title: Sr. Director, Systems 11/10/2023 Date	Name: Maya Kaczmarek Title: Sr. Director, Operations 11/10/2023 Date
V2	MM/DD/YYYY Revised	Name: Title: [MM/DD/YYYY]	Name: Title: [MM/DD/YYYY]

		Date	Date