Cottonwood, Inc.
Policies and Procedures

SECTION: Information Technology **POLICY NO:** 07-001

SUBJECT: Data Governance

EFFECTIVE DATE: April 2023

Background

Data Governance is both an organizational process and a structure. It encompasses the people, processes, and information technology required to create a consistent and proper handling of an organization's data across the business enterprise. It does this through the systematic creation and enforcement of policies, roles, responsibilities, and procedures.

Purpose

The Data Governance Policy addresses the overall management of the accessibility, integrity, and security of data used at Cottonwood, Inc. The purpose of the current Data Governance Policy is to achieve the following:

- Establish appropriate responsibility.
- Establish guidelines for ensuring that the organization's data and information assets are managed consistently and used properly.
- Develop best practices for effective data management and protection.
- Ensure compliance with applicable laws and regulations.
- Ensure data trail is effectively documented within processes associated with accessing, retrieving, exchanging, reporting, managing, and storing data.

Scope

This policy creates a data governance framework to support the consistent and appropriate management of Cottonwood, Inc. data. It establishes the rules, roles, and responsibilities related to the management, utilization, maintenance, access and protection of all data.

- Applies to all data used in the administration of Cottonwood, Inc. (e.g. consumer-related, financial, personnel, donor, customer, government contract)
- Covers, but is not limited to, data in any form, including print, electronic, audio visual, backup and archived data.

Rules

Data Access

The IT staff in concert with Management staff shall be responsible for implementing procedures for granting access to Departmental and Protected Health Information (PHI). **(Policy 07-005 Computer Environment Security)**

Department Directors will determine the need to know for each department. Data shared between Departments will be determined by the concerned Directors or

Management Team. **(Policy 07-005 Computer Environment Security, 3. Securing the Data, Section E.)**

An employee's authorized access to electronic Protected Health Information shall be based upon the minimum necessary informational needs of that employee. **(Policy 05-048 Privacy of Protected Health Information, Pg 75, 4. Information Access Management, b. Access Authorization, c. Access Establishment and Modification)**

Appendix A identifies those classes of Cottonwood, Inc.'s employees who need access to Protected Health Information to carry out their duties and, for each of those classes, the category or categories of Protected Health Information to which access is needed and any conditions appropriate to that access. **(Policy 05-048 Privacy of Protected Health Information, Pg 91, Appendix A Identification of Workforce Members' Access to Protected Health Information)**

Failure of an employee to comply with that access or those conditions will result in disciplinary action up to and including termination of employment.

Data Usage

Authority to read, create, update, and externally disseminate data is enabled for the employees who need each level of permission and understand the relevant Protected Health Information laws. **(Policy05-048 Privacy of Protected Health Information, Page 21, Section C. Use and Disclosure of Only the Minimum Necessary Information, Page 74, Section 3 Workforce Security)**

Employees must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes.

Failure to comply with the Data Usage Policy will be considered in violation of Cottonwood's Code of Conduct and may be subject to disciplinary action or to legal action if laws have been violated.

Data Integration

Well documented data that is easily accessed may be integrated more readily into an existing project or data, reducing redundant work and adding value.

Data governance should always be approached from a collaborative (user) perspective. The Tech Steering Committee (TSC) shall be comprised of representatives from Finance, Human Resources, IT and departmental super-users as needed who are tasked with establishing Cottonwood's strategic technology priorities, as well as a governance framework to support projects and initiatives.

Data Integrity

Data integrity refers to the validity, reliability, and accuracy of data. Ensures that Cottonwood's departments have access to data they can rely on. **(Policy 05-048 Privacy of Protected Health Information, Page 81, 3. Integrity of Electronic Protected Health Information)**

Creates business processes underneath the data to validate accuracy, manage changes or updates to datasets, and track the evolution of data across the pipeline.

Data shall be retained and disposed of in an appropriate manner in accordance with Cottonwood, Inc.'s Recordkeeping Policy (Policy 05-030, Policy 04-022)

Roles / Responsibilities

Data Administrator

Oversees the implementation of the entire data governance program. The Data Administrator takes initiative and makes decisions for the entire organization. The Data Administrator is accountable for the state of the data as an asset.

- CEO / Administrator of Services

Data Steward

Ensures that the authority to read, create, update, and externally disseminate data is enabled for the employees who need each level of permission and understand the relevant PHI laws. The Data Steward has accountability for the day-to-day management of data in the organization and acts as a bridge between business and IT so that business users can access the right data.

- CFO / Finance Manager
- Human Resources Director / HR Coordinator
- Support Services Director / Records Management Specialist
- Director of CDDO Administration
- Residential Director / Residential Coordinator II
- Work Services Director / Data Assurance Coordinator
- Life Enrichment Director / Retirement Coordinator / Work Enrichment Coordinator / CORE Coordinator
- Joblink Director / JobLink Coordinator
- Health Support Nurse Manager / Health Support Clerk
- CR&D Director / Design & Event Coordinator

Data Custodian

Deals with the movement, security, storage, and use of data. The Data Custodian is typically someone in the IT department responsible for implementing the technical requirements specified by the Data Steward.

- Information Technology Manager / Database Developer

Data User

Uses data in their daily work and has access to the data necessary to perform their roles and responsibilities. Data Users have a responsibility to follow established guidelines for accessing, sharing, and updating data as well as participate in activities that define data for use.

Review Process

This Policy will be reviewed and updated yearly from the approval date, or more frequently if appropriate.

Contacts

A comprehensive up to date list of applicable contacts is available on the shared multiuser drive: S:\Data Governance Contacts.pdf

Appendix A: Resources

POLICY NO	NAME	LOCATION
07-001	Data Governance	Intranet
07-002	Cybersecurity Awareness Training	Intranet
07-003	Account Passwords	Intranet
07-004	Computer Internet and E-Mail use	Intranet
07-005	Computer Environment Security	Intranet
07-006	Cybersecurity Incident Response Plan	Intranet
02-016	Electronic Documentation and Signature Policy	Intranet
02-022	Legal Requirements	Intranet
02-033	Social Media	Intranet
04-015	EIV – Use and Safeguards	Intranet
04-022	Retention and Destruction of Administrative / Financial Records	Intranet
04-023	Confidentiality of Administrative Records	Intranet
05-028	Confidentiality of Consumer Documents (30-63-29)	Intranet
05-030	Case Records Maintenance (30-63-29)	Intranet
05-048	Privacy of Protected Health Information (pgs. 73-92)	Intranet
20-018	Computer Use and Security – Work Floor	Intranet

Appendix B: Definitions / Terminology

TERM	DEFINITION
Access	ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource
Data	information collected, created, or maintained by Cottonwood, Inc.(e.g. consumer-related, financial, personnel, donor, customer, government contract)
Integrity	property that data or information have not been altered or destroyed in an unauthorized manner.
Protected Health Information (PHI)	any health information maintained by Cottonwood, Inc. that is individually identifiable except: (a) employment records held by Cottonwood, Inc. in its role as an employer; and, (b) information regarding a person who has been deceased for more than fifty (50) years.