Authorization to Share and/or Exchange Data With the National Council on Aging (Rev. 9/12/2022)

Instructions: Email completed form to angelica.herrera-venson@ncoa.org for the National CDSME Database and the National Falls Prevention Database to authorize data transfers/exchange with the National Council of Aging.

* * *

This Mutual Confidentiality Agreement ("Agreement") is made this {EFFECTIVE DATE} by and between National Council on Aging, Inc. (hereinafter referred to as "NCOA") with principal offices at 251 18th St S Suite 500 Arlington, VA 22202, {Grantee/Network /Name of Organization}, having a place of business at {Grantee/Network Name ADDRESS}; and {Vendor/Third Party}, having a place of business at {ENTITY ADDRESS}.

I, {Name of Representative}, on behalf of {Grantee/Network Name}, authorize {Name of Vendor / Third Party Holding Data} to share and/or exchange evidence-based program activity data pertaining to {Grantee/Network Name} with the National Council on Aging (NCOA) with the following stipulations and conditions.

I. Grantee / Network Account Details

The present agreement pertains to data to be shared and/or exchanged between NCOA and _____ (Grantee / Network Account, as named in either the National CDSME or Falls Prevention Database). Grantee /Network Account #: _____.

II. Selected Programs and Date Ranges

Check the box to indicate the database to which you are authorizing data transfer to NCOA.

☐ **National CDSME Database**

Specify the names of the programs for which you wish to share data, and the corresponding date range. Indicate the start and end dates for workshops and participants.

Program Name	Date Range of Workshops to Transfer: Use End Dates of Workshops, as reference __/__/__ to __/__/__	Frequency (e.g. monthly, quarterly, yearly, other)

_____ (**Initials**) We would like data to be shared with the National CDSME Database indefinitely, unless otherwise notified in writing by an authorized representative from our organization to cease data transfer.

☐ **National Falls Prevention Database**

Specify the names of the programs for which you wish to share data, and the corresponding date range. Indicate the start and end dates for workshops and participants.

Program Name	**Date Range of Workshops to Transfer: Use End Dates of Workshops, as reference __/__/__ to __/__/__**	**Frequency (e.g. monthly, quarterly, yearly, other)**

_____ (**Initials**) We would like data to be shared with the National Falls Prevention Database indefinitely, unless otherwise notified in writing by an authorized representative from our organization to cease data transfer.

III. Approval for Bidirectional Data Exchange

When first establishing a connection for data sharing, oftentimes, the vendor needs to pull data from the National CDSME or Falls Prevention Databases to establish a baseline and cross-reference items, such as host organization or implementation site ID#'s, and other data elements. This ensures that future data imports do not create duplicates or overwrite existing data. The vendor may need occasional exports of your data to help with cross-validation and for quality assurance.

A grantee/network may also wish to have data exported from the National CDSME or Falls Prevention Database for other reasons, including for the purpose of ensuring that their vendor database includes historical data and that the two databases mirror each other. Or the organization may wish to have all of their data (historical and present) shared with a vendor at the conclusion of their active grant cycle to continue program monitoring exclusively with the vendor or other entity. This can take place during or at the end of the grant cycle.

Please initial the following statement, where appropriate, to indicate the circumstances under which you approve your network's data to be shared with your vendor from the National CDSME or Falls Database.

____ (**Initials**) I agree that {Vendor/Third Party} may receive data files from the National CDSME or Falls Databases pertaining to the programs and account noted in Section II, for the purpose of cross-validation and quality assurance in the early stages prior to commencing data importing from the vendor/third party to the National CDSME or Falls Databases. This may include historical data for workshops with end dates prior to the start date of the network's active grant cycle.

____ (**Initials**) I agree that {Vendor/Third Party} may receive data files from the National CDSME or Falls Databases pertaining to the programs, account, and workshop end dates noted in Section II, at the conclusion of the grant cycle to ensure that the two databases mirror each other.

____ (**Initials**) I agree that {Vendor/Third Party} may receive data files pertaining to the programs, account, and workshop end dates noted in Section II, for the purpose of

cross-validation and quality assurance at any time during the time frame indicated in Section II, at the request of the grantee/network or vendor.

IV. Adherence to Data Privacy and Security Standards

All data associated in this exchange is de-identified, and no protected health information (PHI), such as Medicare numbers, names, Dates of Birth, or medical histories exist in our records, thereby complying with the Health Insurance Portability and Accountability Act (HIPAA) regulations.

1.0 Treatment of Non-Public Data or Confidential Data Non-Public Data (NPI) or Confidential data, as identified by the Data Classification Policy, should be handled by NCOA employees and contractors in a manner compliant with NCOA's standards applying specific security controls to protect this data.

1.1 Examples of NPI or Confidential Data
The following list is not intended to be exhaustive, but provides NCOA with guidelines on what type of information is typically considered NPI or Confidential. NPI or Confidential data can include:

- Employee or customer social security numbers or personal information
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)
- Customer data
- Date of Birth
- Participant Zip Code
- Program Leader's names, emails, and phone numbers
- Company financial data (if company is closely held)
- Product and/or service plans, details, and schematics,
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

1.2 Storage
NPI or Confidential data must be removed from desks, computer screens, and mobile data devices that utilizes flash memory to store data (often called a USB drive, flash drive, or thumb

drive) and common areas unless it is currently in use. NPI or Confidential data should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

1.3 Transmission & Encryption
Passwords must be used when transmitting NPI or Confidential data, regardless of whether such transmission takes place inside or outside NCOA's network. NPI or Confidential data must not be left on voicemail systems, either inside or outside NCOA's network, or otherwise recorded. All data files must be submitted via NCOA's Safe-File Transfer Program (S-FTP) system, https://ncoa.moveitcloud.com/. NCOA will set up an account for the vendor.

1.4 Destruction
NPI or Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: Cross-cut shredding is required.
- Storage media (CD's, DVD's): Physical destruction is required.
- Hard Drives/Systems/Mobile/Cloud Storage Media: Physical and/or logical destruction is required. If physical destruction is not possible, the IT Manager must be notified.
- Storage of NPI data on removable media must comply with the Information Security Policy.

1.5 Incident management and notification:
In case of a breach, or inadvertent or intentional acquisition of client data, the vendor must notify NCOA within 24 hours in writing about the nature and scope of the breach.

2.0 Use of NPI or Confidential Data
The following applies to how users must interact with National Council on Aging NPI or confidential data:

- Users must be advised of any NPI or Confidential data they have been granted access. Users must only access NPI or Confidential data to perform his/her job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of NPI or Confidential data. Users must protect any NPI or Confidential data to which they have been granted access and not reveal, release, share, email without the use of passwords, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor. Users must report any suspected misuse or unauthorized disclosure of NPI or Confidential data immediately to his or her supervisor. If NPI or Confidential data is shared with third parties, such as contractors or vendors, a non-disclosure agreement must govern the third parties' use of NPI or Confidential data.
- If NPI or Confidential data is shared with a third party, NCOA must indicate to the third party how the data should be used, secured, and, destroyed.
- NPI or Confidential data must be removed from documents unless its inclusion is absolutely necessary.

- NPI or Confidential data must never be stored on non-company-provided machines (i.e., home computers).
- If NPI or Confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

3.0 Security Controls for NPI or Confidential Data

NPI or Confidential data requires additional security controls in order to ensure its integrity. NCOA requires that the following guidelines are followed:

- Passwords: Passwords must be used for Confidential data transmitted internal or external to NCOA.
- Physical Security: Systems that contain NPI or Confidential data, as well as NPI or Confidential data in hardcopy form, should be stored in secured areas with access controls that secure this data.
- Printing: When printing NPI or Confidential data the user should use their best efforts to ensure that the information is not viewed by others. Printers that are used for NPI or Confidential data must be located in secured areas.
- Faxing: When faxing NPI or Confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the NPI or Confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving NPI or Confidential data must be located in secured areas.
- Emailing: NPI or Confidential data must not be emailed inside or outside the company without the use of passwords.
- Mailing: If NPI or Confidential data is sent outside NCOA, the user must use a service that requires a signature for receipt of that information. When sent inside NCOA, NPI or Confidential data must be transported in sealed security envelopes marked "Confidential."
- Public Sites & Social Media: Further, client data must not be shared, as raw data, or even as high-level aggregate findings on any public domain, Website, or social media, without the written consent of either ACL or the client/grantee/network.
- Discussion: When NPI or Confidential data is discussed it should be done in non-public places, and where the discussion cannot be overheard.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date written above.

_____	_____
National Council on Aging	{Vendor/Third Party}
Signature:	Signature:
_____	_____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

_____

{ENTITY/Organization Name}