**DATA USE AGREEMENT FOR THE NATIONAL COUNCIL ON AGING, CENTER FOR HEALTHY AGING**

This Data Use Agreement (“Agreement”) is entered into by and between the National Council on Aging (“Covered Entity”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“Data User”) and is effective as of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“Agreement Effective Date”) **and will remain effective for one year unless changed or cancelled by either party.**

The National Council on Aging manages data for chronic disease self-management education programs and evidence-based falls prevention programs for current and former recipients of grant funding from the Administration for Community Living / Administration on Aging (ACL/AoA). This agreement provides an overview of the guidelines, including restrictions, for the proper use of the national data for research and evaluation activities.

1. **Obligations of Covered Entity**
2. Covered Entity agrees to share the following information with Data User (the “Limited Data Set”):

*Chronic Disease Self-Management Education Program Data*: □ Yes □ No

*Falls Prevention Program Data*: □ Yes □ No

1. The Limited Data Set shall not contain any of the following participant identifiers: name, postal address information (other than state), Dates of Birth, electronic mail address(es), social security numbers, and Driver’s License.
2. The Limited Data Set shall contain the following data fields to enable the Data User to perform proposed research. The following also details specifications of the data, e.g., a date range, workshop type, geography, or other.

[List of data fields]

[List of other specifications]

1. The Limited Data Set shall be provided to the Data User in the following format, using encryption tools outlined in ***NCOA’s Client Data Sharing and Protection Agreement*** (Appendix A) to ensure that client’s data is protected while in transit.

□ .csv □ .xls □ .sav □ Other (specify: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

1. **Obligations of Data User**
2. The Data User must provide a Curriculum Vitae to the Covered Entity for self and key contributors.
3. *Performance of Activities.* Data User may use and share findings resulting from analysis of the Limited Data Set received from Covered Entity only in connection with the performance of the evaluation/research activities (“Activities”) described below
4. NCOA requires a high-level overview of the goals, objectives, research designs/approach, measures, and any plans to merge or link NCOA data sources to other data sources (e.g. national health data sources) written in laymen’s terms in the section below. Attach additional information, if needed.
5. An Institutional Review Board (IRB) approval document from the Data User’s institution or other trusted entity is required, if applicable to the Data User’s institution. Please attach a copy.
6. *Value and Research Activity:* The research activity must add value and fill a gap in the scientific literature. In the space provided below, please specify how the proposed research activity or analysis will be used to fill a gap in the scientific literature. Include citations.
7. *Notice of Expected Publication or Dissemination.* The Data User must receive written approval by the Covered Entity prior to submitting and/or publishing findings developed with information derived from the Limited Data Set. This includes submission of a manuscript to peer-reviewed journals, abstracts for poster or oral presentations at conferences, or the sharing of findings with the media or other purposes. If the Data User’s findings are accepted by a journal or conference for presentation, publication, or other form of dissemination, the Data User must provide notice to the Covered Entity within 30 days after the acceptance.
8. *Review of findings.* The Data User is required to provide the Covered Entity with an opportunity to review manuscripts or other products emanating from the Limited Data Set at least 30 days prior to time of dissemination through any venue previously noted.
9. *Sharing Reconfigured Dataset.* The Data User shall provide the Covered Entity with the updated data set, including data transformations, coded data, labels, syntax and associated manipulations of the data performed during the conduct of the research proposed.
10. *Acknowledgment.* All products developed with information derived from the Limited Data Set will acknowledge the Administration for Community Living/Administration on Aging as the primary funding source and include a statement that reads “Opinions expressed do not necessarily represent official Administration for Community Living/Administration on Aging policy” on any publications/materials. Acknowledgment of NCOA staff, or listing as co-authors, is also acceptable in accordance to guidelines clarified in the International Committee of Medical Journal Editors and authorship guidelines established by the HHS Office of Research Integrity.
11. *Limitations*. The Data User may not use the Limited Data Set for any research or evaluation not explicitly outlined in this agreement. If the scope of research requires revision, a written amendment should be made describing those changes to the original agreement. Data User shall not use or further disclose the Limited Data Set except as permitted by this Agreement.
12. *Permitted Access to Limited Data Set.* Data User shall limit the use or receipt of the Limited Data Set to the following individuals or classes of individuals, such as temporary research assistants or fellows under the Data User’s supervision, who need the Limited Data Set for the performance of the Activities. NCOA should be notified of additions/changes to the list within 15 days of changes.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Affiliation** | **Email address** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. *Assurances of Data Users Non-Employee Agents.* Data User shall not disclose the Limited Data

Set to any non-employee agent or subcontractor of Data User except with the prior written consent of Covered Entity. Data User shall ensure that any agents, including subcontractors, to whom it provides the Limited Data Set, agree in writing to be bound by the same restrictions and conditions that apply to Data User with respect to the Limited Data Set.

1. *Data Privacy & Security Safeguards.* Data User, including those permitted access as listed in k. above, shall adhere to ***NCOA’s Client Data Sharing and Protection Agreement*** (Appendix A) to ensure that client’s data is protected while in possession or in transit.
2. **Agreement**

If the above information is agreeable, please sign and date in the space provided below.

|  |  |  |
| --- | --- | --- |
| Name of Designated Data User: | | Date: |
| Signature: | |  |
| Organization/Institution: | |  |
| Title: | |  |
| Address: | |  |
| E-Mail Address: |  | |
| Telephone: | |  |

If the above information is agreeable, please sign and date in the space provided below.

|  |  |  |
| --- | --- | --- |
| Name of Designated Covered Entity: | | Date: |
| Signature: | |  |
| Organization: | | *National Council on Aging* |
| Title: | |  |
| Address: | |  |
| E-Mail Address: |  | |
| Telephone: | |  |

APPENDIX A.

The National Council on Aging Client Data Sharing and Protection Agreement

**Policies and Procedures for Sharing and Protecting Client Data**

1. **HIPAA Compliance**

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

**2.0 Treatment of Non-Public Data or Confidential Data**

Non-Public Information (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.

**2.1 Examples of NPI or Confidential Data**

The following list is not intended to be exhaustive, but provides NCOA and partners 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)

**2.2 Storage**

NPI or Confidential data must be removed from desks, computer screens, and mobile data devicesthat 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) at all times, with the key, keycard, or code secured.

**2.3 Transmission & Encryption**

The file should be password-protected and sent to NCOA through the PARTNER’s own IT department’s recommended encryption methodology or alternatively use NCOA’s S-FTP solution (MoveIt). Any file sent to NCOA outside the secure protocol and preferred NCOA format will be deleted and the PARTNER will be notified accordingly.

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.

**2.4 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.

**2.5 Incident management and notification:**

* In case of a breach, inadvertent or intentional acquisition of client data, the PARTNER must notify NCOA within 24 hours in writing about the nature and scope of the breach and plans to remediate. Conversely, NCOA agrees to notify the PARTNER within 24 hours in writing about the nature and scope of a breach that may occur at NCOA and plans to remediate.

**3.0 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).
* NPI or Confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

**4.0 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.
* **Discussion**: When NPI or Confidential data is discussed it should be done in non-public places, and where the discussion cannot be overheard.