Privacy and Data Security

Practices & Procedures

National CDSME Program Database

National Falls Prevention Program Database

July 20, 2018

Safeguarding program data in the National CDSME and Falls Prevention Databases is everyone's responsibility. This document summarizes NCOA's recommended practices for ensuring the security and privacy of participant data, data sharing, and the Salesforce security model employed by NCOA.

I. Storing and Discarding Paper Files and Electronic Data

To meet privacy and security standards, grantee/network partners should:

- Store completed data collection forms in a secure, locked cabinet when not in use
- Enter data into a secure, password protected database, such as the National CDSME and Falls Evidence-based Program prevention databases
- The following documents can be destroyed <u>immediately after entering data into the database</u>:
    - Program Information Cover Sheet
    - Attendance Log
    - Participant Information Survey (and Post Session Survey for Falls programs)
    - Host and Implementation Site Organization Information Form
- Keep ELECTRONIC copies of data for at least 3 years past last report date associated with grant (e.g. grant period end date of 2/28/2017 → should keep data at least through 2/27/2020). Once the data is entered into the respective national database, NCOA is responsible for maintaining that data for at least 3 years.
- Have appropriate program staff complete a Non-Disclosure Agreement (NDA)
    - A Non-Disclosure Agreement is an acknowledgement that participant information should not be shared with others and should be safeguarded appropriately

- Grantee lead or the designee for data collection must keep Non-Disclosure Agreement in locked secure storage or store electronically scanned copies in a secure, password protected database for 3 years.

II. Provide Staff with Adequate Training and Require Non-Disclosure Agreements

Centralize data management as much as possible and create accountability for securing the safety of your program and participant-level data.

Limit the number of users accessing the National CDSME & Falls Prevention Databases to a manageable number. There is something to be said about having "too many cooks in the kitchen." Your data management processes should include quality assurances and controls.

All staff handling data collection forms or entering program data should be adequately trained and complete a non-disclosure agreement (NDA).

Access a copy of NDA's for each program on our resource pages here:

Falls Prevention:

Non-Disclosure Agreement for Data Collection Personnel (English)

CDSME:

Non-Disclosure Agreement (English)
Spanish Non-disclosure Agreement (Spanish)

You do not need to provide any additional training for personnel who have already undergone privacy and security training through their agency.

NCOA has developed a basic PowerPoint that is available on its website for distribution to those who need training. We recommend that when you orient your personnel to the data collection forms that you also incorporate the slides from this PowerPoint: Power Point Presentation: Privacy and Security Basics for Falls Prevention Evidence-Based Programs.

In addition, you can use this handout to provide further guidance for managing and securing your program data files.

III. Handling Sensitive Data and Complying with HIPAA Regulations

If you are collecting Personal Health Information (PHI) or Personally Identifiable Information (PII) data as part of your ACL grant requirements or as part of any other complementary evaluation efforts, please consider the following to ensure you meet HIPAA requirements associated with the Privacy Act.

The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI).

- Evidence-based program data may, in some cases, contain sensitive PHI/PII data that is protected by Privacy Act:

    - Personal Health Information (PHI) – physical/mental health condition
    - Personally Identifiable Information (PII) – name, zip code

- Let your respective IT department guide your security protocols accordingly

- Use National CDSME and Falls Prevention Databases or other secure database
- When sharing data with any other partner, follow the guideline in Section IV below
- Let the NCOA database management team know as soon as someone leaves so that they can deactivate their account
- Security discard forms (such as by shredding) once entered into secure database

IV. Sharing Participant-Level Data between Vendors, Grantees/Data Users and NCOA

It's always preferable that you provide summaries to external partners in aggregate form – no participant-specific data. However, when sharing participant-level data that may contain sensitive data (PII or PHI), it is highly recommended that you follow a number of basic practices:

1) De-identify data if used in non-summarized form

- Strip data of identifiers, such as zip codes, phone numbers, names, birthday/ages, and any other identifier that you may be collecting in conjunction with program data. There is a list of 18 recognized identifiers. For a summary of the list, see: https://cphs.berkeley.edu/hipaa/hipaa18.html.

2) Set up a Data Use Agreement

- A Data Use Agreement (DUA) is a contractual document used for the transfer of data that has been developed by nonprofit, government or private industry, where the data is nonpublic or is otherwise subject to some restrictions on its use.
- If you are working with a research/academic institution, an IRB may cover only some aspects of the data sharing and data security requirements. With research partners wanting full data exports (or excerpts of it) containing detailed case-level data with PHI or PII, you definitely want to set up a DUA. It is advisable that you set up a DUA even when de-identified data is shared with a research partner so that you spell out expectations about how the analyses, findings, and scrubbed / manipulated data files will be shared back with your organization

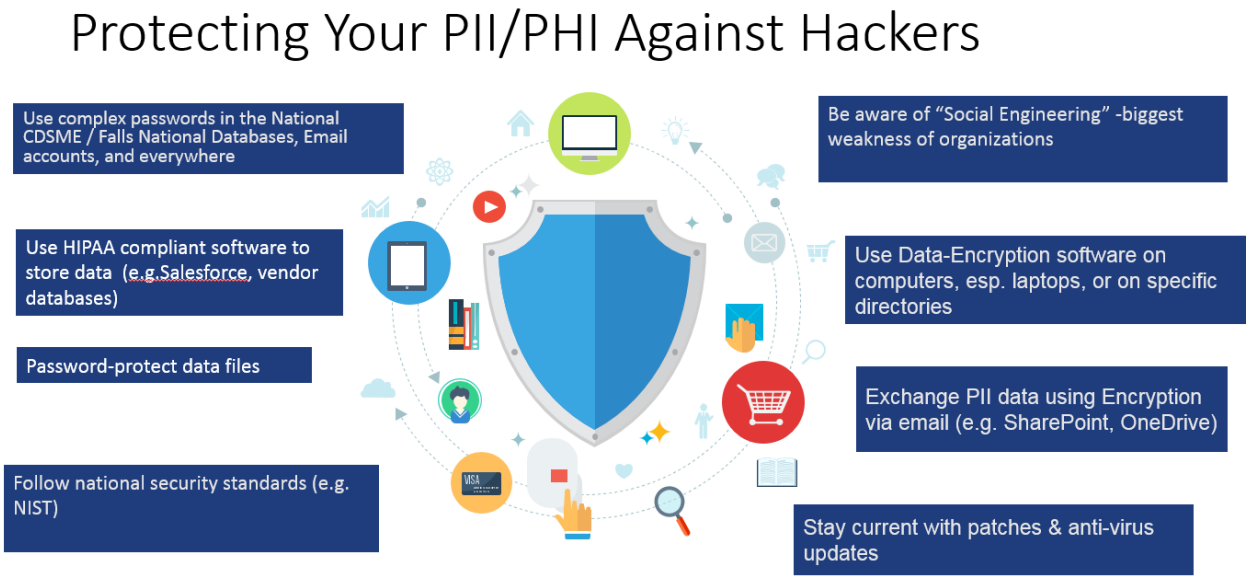
once the research/analyses is complete, clarify on whether you'll be given an opportunity to review publications or other reports before they are releases, and indicate how your organization will be acknowledged on those reports. Learn more about working with research institutions (https://privacyruleandresearch.nih.gov/)

- When sharing aggregate data to funders, other community partners, or the media, you do not need a DUA.

3) Used Various Tools to Ensure the Safe Transmission of Data

Follow standard practices for transmitting data to external parties that may contain PHI or PII sensitive data, and that is not de-identified or in aggregate/summary form:

- Grantees and other partner organization are urged to use email encryption software, and should explore their options with their IT support staff, as costs, complexity, and compatibility may vary.
- Password protected your files using the tools provided by the application, such as Microsoft Word's Protect Document -> Encrypt with Password option (an example of what NCOA uses internally in conjunction with other methods).
- Files can be shared via Safe File Transfer Protocol (SFTP) server when possible.
- NCOA currently encrypts files with external users in one of two ways. Grantees and partners may wish to follow this approach to data sharing:
    - Via OneDrive or SharePoint. The receiver is required to sign-in with a Microsoft account to access file. Office 365 is compliant with several security certifications. This information can be found on the **Office 365 Security site.**
    - Through direct encrypted emails to other users. We type the word "encrypt" in the Subject line of the email message. The receivers will be required to sign in using a Microsoft account and password before they can read the email.
    - NCOA laptops use BitLocker to encrypt the hard drives of laptops. Additional encryption software may be required based on contract requirements. These are options that grantees/network partners can follow.
- As with most organizations, human error is our greatest concern. In this case, password sharing and weak passwords are the largest risks. We require minimum 8 characters and a mix of letters, case and numbers. This applies to your email account, your Salesforce / national database account, and any other system involved in your data management and transfer.
- Be wary of "social engineering" – it's the biggest weakness among organizations. These are disguised attacks in the form of emails from hackers who manipulate people into offering up personal information or enticing users to click on links, which then permit their entry into your computer system.



V. What is Salesforce's Data Security Model?

- The National CDSME Database and National Falls Prevention Database are hosted on the Salesforce.com platform. Therefore, they are automatically covered by the security guarantees that Salesforce provides (see trust.salesforce.com) across their entire platform. The additional methods listed above ensure that our legitimate users only see their own organization's data.
- Salesforce is fully HIPAA compliant (security features – TRUST site) trust.salesforce.com
- Non-NCOA users are restricted from accessing data by:
    - global limits on their user license types
    - record sharing policies set by NCOA
    - record type restrictions
    - field level security
- To provide a security model that satisfies numerous, unique real-world business cases, Salesforce provides a comprehensive and flexible data security model to secure data at different levels. All these data security models are strictly followed by the NCOA on the Databases.
- Please contact the NCOA database management team for additional documentation and details on the Salesforce security features.