national council on aging

Privacy & Security Resource

For Grantees and Users of HAPID®

Updated on 8/22/2024

Disclaimer: This resource is not meant to be exhaustive or complete for privacy & security training for your organization but is only meant as a starting point.

Outline

1. Overview
2. How to Use This Resource
3. PII & HIPAA & PHI
4. Access & Permissions in HAPID® for Grantee Accounts / Users
5. Further resources and information

How to Use this Resource

How to Use this Resource

- This is not meant to be an exhaustive resource.
- All organizations are unique and some may be subject to stricter requirements to protect data than others
  - Healthcare providers
  - Universities (may be subject to additional requirements set forth by the Institutional Review Board.)
- This resource can be used as a template that you can build on according to the needs of your organization. Please feel free to customize this PowerPoint according to your institutional requirements.

Overview

Overview

- Background on Privacy Act
- Intended audience for this presentation
- Security best practices for documents for staff/contractors/volunteers

Privacy Act of 1974

- Protects records that can be retrieved by personal identifiers such as a name, social security number, or other identifying number or symbol.
- Created in response to concerns about how the use of computerized databases might impact individuals' privacy rights.
  - Requires government agencies to show individuals any records kept on them
  - Requires agencies to follow "fair information practices" when gathering and handling personal data.
  - Places restrictions on how agencies can share an individual's data with other people and agencies.
  - Allows individuals the ability to sue the government for violating of these provisions
- http://www.hhs.gov/foia/privacy/

Intended audience for this presentation

- Anyone involved in the collection, handling and/or data entry participant data in CDSME or Falls Prevention programs, regardless whether that data is in paper form or electronic.
- Any frontline staff, such as Facilitators, Instructors, or Workshop coordinators that may be involved in tracking participant attendance or collecting pre- or post-test surveys.
- Anyone entering data into HAPID or viewing or exporting data from its reports or dashboards.
- Anyone involved in the management of sensitive information, Personally Identifiable Information (PII), or protected health information (PHI), you need to unauthorized access/disclosure, theft, loss, and improper disposal protocols.
- Anyone who is intending to collect additional data from participants beyond ACL OMB form requirements.

Additional considerations

- While the official database for the Falls and CDSME Prevention programs collected in HAPID does not collect sensitive data such as Date of Birth, medical records #'s, SS#'s, Medicare #'s, participant names, or anything else that would fall under PII or PHI, etc., it is important to address some basic concepts around protecting the data that is collected from evidence-based program participants.

- In addition, some of you may be collecting additional data alongside the EBP data, such as their names, phone #'s, and possibly connecting data with other medical records (in particular, for healthcare organizations). Some of you conducting research, may also be collecting additional fields at your university. Hence, it's important to train your staff on appropriate protections for data being collected or encountered in this process.

Recommended Training

- Training for program coordinators and program implementers
  - The rights of individuals participating in evidence-based programs
  - The appropriate protection of PII shared by program participants at the workshop level
  - The appropriate storage and transfer of participant forms

- Training for individuals completing data entry and data transfer
  - The appropriate protection of PII shared by program participants at the workshop level
  - The appropriate storage, transfer, and destruction of data forms
  - Security requirements for electronic data transfer, storing, and degaussing (destruction)

Disclosure

- No agency or person shall disclose:
  - any record
  - by "any means of communication"
  - to any person or another agency
  - without a written request or prior written consent of the individual to whom the record pertains

- “Any means of communication” includes oral (phone, in-person), written, and electronic (emails, faxes, texts, tweets, pins, etc.)

Safeguarding PII

- Must always be treated as “FOR OFFICIAL USE ONLY” and must be marked accordingly
- Applies not only to paper records but also includes email, faxes, etc., which must contain the cautionary marking “FOR OFFICIAL USE ONLY”
- Should be stored in locked filing cabinets or other secure containers to prevent unauthorized access
- Electronic records must be password protected and be transferred via encrypted email

Transporting PII

- Hand carrying
  - Use a cover sheet or large envelope to shield contents
- Using mail
  - Use manila or white envelopes
  - Mark the envelope to the attention of the authorized recipient
  - Never indicate on the outer envelope that it contains PII
- Using email
  - Password protect personal data placed on shared drives, the Internet, or the Intranet
  - Use encrypted email
  - Do not send PII to a personal, home, or unencrypted e-mail address
  - Announce in the opening line of the text (NOT the subject line) that FOUO information is contained

Disposing of PII

- A disposal method is considered adequate if it renders the information **unrecognizable** or **beyond reconstruction**.

- Disposal methods may include:
  - Burning
  - Melting
  - Chemically decomposing
  - Pulping
  - Pulverizing
  - Shredding
  - Mutilating
  - Degaussing (erasing from magnetic field or disc)
  - Deleting/emptying recycle bin

Recommended Practices

- Take privacy protection seriously
- Respect the privacy of others
- Ensure messages, faxes, and emails that contain personal information are properly marked and email is encrypted
- Don’t share PII with individuals who are not authorized
- Have appropriate transfer, storage, and disposal protocols in place for PII
- Do not email PII to personal, home, or unencrypted accounts
- Use and customize the Group Leader Script to advise all participants of their right to consent or refuse use of data about them

Recommended Practices

- All individuals involved in providing evidence-based programs must sign **Non-Disclosure Agreements**
- All individuals involved in data collection, data transfer, and/or data entry must sign Non-Disclosure Agreements
- Non-Disclosure Agreements should be maintained for three years after the end of the grant and stored by the grantee or the grantee's designee for data collection/data entry
- Non-Disclosure Agreements do not contain PII, so they can be faxed, e-mailed, or mailed without encryption or privacy restrictions

Non-Disclosure Forms

Your staff can use the following Non-Disclosure Agreement. NCOA does not need a copy. This is for your organization's internal use and recordkeeping. You can adapt the form to your needs.

Scroll to Section "2. Staff training and non-disclosure agreements"

https://www.ncoa.org/article/privacy-and-data-security-practices-healthy-aging-programs-integrated-database

Organizational Best Practices

Protecting Your PII/PHI Against Hackers

- Use complex passwords in the National CDSME / Falls National Databases, Email accounts, and everywhere
- Use HIPAA compliant software to store data (e.g.Salesforce, vendor databases)
- Password-protect data files
- Follow national security standards (e.g. NIST)

- Be aware of “Social Engineering” -biggest weakness of organizations
- Use Data-Encryption software on computers, esp. laptops, or on specific directories
- Exchange PII data using Encryption via email (e.g. SharePoint, OneDrive)
- Stay current with patches & anti-virus updates

Good Practices for Collecting Data Online for Virtual/Remote Programs

- If collecting data through SurveyMonkey, GoogleForms, RedCap, or other online tools, here are a few tips for keeping data safe and having full disclosure.
- The first page of each survey should introduce the purpose of the survey, who is running the survey, who to contact, and who will have access to any data you collect. *They should be notified whether their name or other PII will be connected to their responses and level of confidentiality and anonymity they can expect.*
- Those managing the online survey should download exports of that data only onto safeguarded servers and computers.
- This data should be entered into a secure database within 30 days, such as HAPID, as required of ACL grantees. You can keep original survey data for up to 3 years on other safe computers (pass-word protected file, pass-word protected computer).
- If downloaded data from these data collection tools is to be shared with other staff or partners in, be sure to email it using Encrypted methods/tools.
- It's helpful to introduce links to online surveys at the first workshop session and at the last session, via Zoom or other web tool, so that participants recognize the link, have greater trust, and this increases response rates.

HIPAA & PII & PHI (18 identifiers)

HIPAA & PHI (18 identifiers) & PII

HIPAA

- **Covered Entities & Business Associates**
  - HIPAA Privacy Rule
    - Covers all PHI
  - HIPAA Security Rule
    - Covers ePHI

  - Always defer to the statutes and laws in your own state when considering patient privacy if those laws are stricter than HIPAA. If those laws are not stricter than HIPAA, please make sure you're in compliance with HIPAA.

  - For more information on HIPAA enforcement: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

PII & HIPAA & PHI (18 identifiers)

PII & PHI

PII is personally identifiable information or any information that could be used to identify a person.

- PHI is part of PII and protected under HIPAA. Any personal identifiable information (PII) when connected to anything health related becomes PHI (personal health information).

PII & HIPAA & PHI (18 identifiers)

PHI – 18 identifiers

- (1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
- (2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
- (C) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- (D) Telephone numbers
- (L) Vehicle identifiers and serial numbers, including license plate numbers
- (E) Fax numbers
- (M) Device identifiers and serial numbers
- (F) Email addresses
- (N) Web Universal Resource Locators (URLs)
- (G) Social security numbers
- (O) Internet Protocol (IP) addresses
- (H) Medical record numbers
- (P) Biometric identifiers, including finger and voice prints
- (I) Health plan beneficiary numbers
- (Q) Full-face photographs and any comparable images
- (J) Account numbers
- (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section [Paragraph (c) is presented below in the section “Re-identification”]; and
- (K) Certificate/license numbers

Source: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

HIPAA & PHI (18 identifiers) & PII

De-identification of PHI

- In order to use any health information that could be tied to a person, you have to first go through de-identification of health information.
  - 2 methods:
    - Safe harbor – de-identification of PHI identifiers
    - Expert determination

How this looks when inputting data into HAPID®

- Never enter in any information that is PHI (any information that falls under the18 identifiers) or PII when entering information about participants in the database unless it has been de-identified.

HIPAA & PHI (18 identifiers) & PII

How this looks when inputting data into HAPID®

- Do not enter:
  - Name of participant
  - DOB
  - participant zip codes with county
  - Email addresses
  - Any other information from the list of identifiers for PHI.

Healthy Aging Programs Integrated Database® | HAPID®

Access & Permissions for Users

HAPID®

Access and Permissions in HAPID®

- For grantee level accounts, only the user accounts under the grantee account have access to the information in the grantee account. Users under the grantee account may also see data from host level accounts. For more information on levels of access given to users of the database, please see the third point.
- For host level accounts, user accounts under the host account can only see workshops that are affiliated with that host account. For more information on levels of access given to users of the database, please see the third point.
- For more information on permissions between Super User and Data Entry users, please see the table in the following slides. Please note that permissions/capabilities of users are subject to change as we work towards adding more functionality to users in the database.
- Please note, administrator/staff from NCOA team will have access to information in all grantee, host, and any other accounts in the database (i.e. non-grantee accounts, etc.)

Table taken from User Manual**

ACTION	SUPER USER	DATA ENTRY
View a listing of active Hosts Organizations and Implementation Sites associated with your Network, Account	YES	YES
View workshops created by you or your team	YES	YES
Create workshops	YES	YES
Edit workshop you or others created	YES	YES
Add/edit/delete participants to workshops created by you or others on your Account	YES	YES
Delete a workshop created by you	YES	YES
Delete a workshop created by someone else	YES	NO
Delete a participant^	Requires Admin Assistance	Requires Admin Assistance
Change the Evidence-based Program/workshop type (e.g., Matter of Balance, Walk With Ease) to another one on an existing workshop record.	May require Admin Assistance	May require Admin Assistance

Always check the latest User Manual for the latest permissions, as this may change:
https://www.ncoa.org/article/how-to-use-the-healthy-aging-programs-integrated-database

Table taken from User Manual

ACTION	SUPER USER	DATA ENTRY
Move a workshop from one Host Org or Implementation Site to another	YES	Requires Admin Assistance or Ask a Super User on your team to do
Move a workshop from one Program Target to another	YES	YES
Create Host organizations & Implementation Sites	YES	YES
Edit or Delete Host organizations & Implementation Sites	YES	NO
Create a Facilitator	YES	YES
Edit a Facilitator*	YES	YES
Delete a Facilitator*	NO	NO
Create a non-ACL Program Target	YES	NO
Create an ACL Program Target	NO	NO
View & Export Reports / Dashboards	YES	NO
Create surveys	Requires Admin Assistance	Requires Admin Assistance

Always check the latest User Manual for the latest permissions, as this may change:
https://www.ncoa.org/article/how-to-use-the-healthy-aging-programs-integrated-database

HAPID®

Security in HAPID®

- **HAPID®** is housed in the Salesforce platform.
  - Comes with standard protections that Salesforce offers.

- Secured login – username & password

- Fulfills the technical requirements for HIPAA:
  - Secured login
  - Users only have access to the information that belongs to them as well as the grantee/organization account.
  - All information that could be PII has been de-identified when it is inputted into HAPID.
  - Only researchers that sign a Data Use Agreement have access to the information in the database and even then, the information on participants is de-identified.

HAPID®

Data Security Model:

HAPID® is 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.

Resources

Resources

HIPAA Basics

- https://www.healthit.gov/topic/privacy-security-and-hipaa/hipaa-basics
- https://www.hhs.gov/hipaa/index.html
- https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers

Security and HAPID

- https://www.ncoa.org/article/how-to-use-the-healthy-aging-programs-integrated-database
- https://www.ncoa.org/article/privacy-and-data-security-practices-healthy-aging-programs-integrated-database

Q & A

Thank you for your time and attention during this presentation.