Module 7: Security & Privacy Training for Volunteer Assisters

Office of Medicaid Eligibility Policy

Medicaid Programs Division

2023

Washington State Health Care Authority

Topics

- Volunteer Assister Access for Health Care Authority (HCA) Community Partners
- Threats
- Information
- Prevention Tactics
- Incident
- Volunteer Assister Access

Volunteer Assister Access for HCA Community Partners

Purpose

- This training provides guidance on Security and Privacy practices for CMS and IRS compliance and to:
  - Establish a baseline of security awareness for working with the Washington Health Benefit Exchange's web portal also referred to as Washington Healthplanfinder.
  - Increase Security and Privacy Awareness.

Security

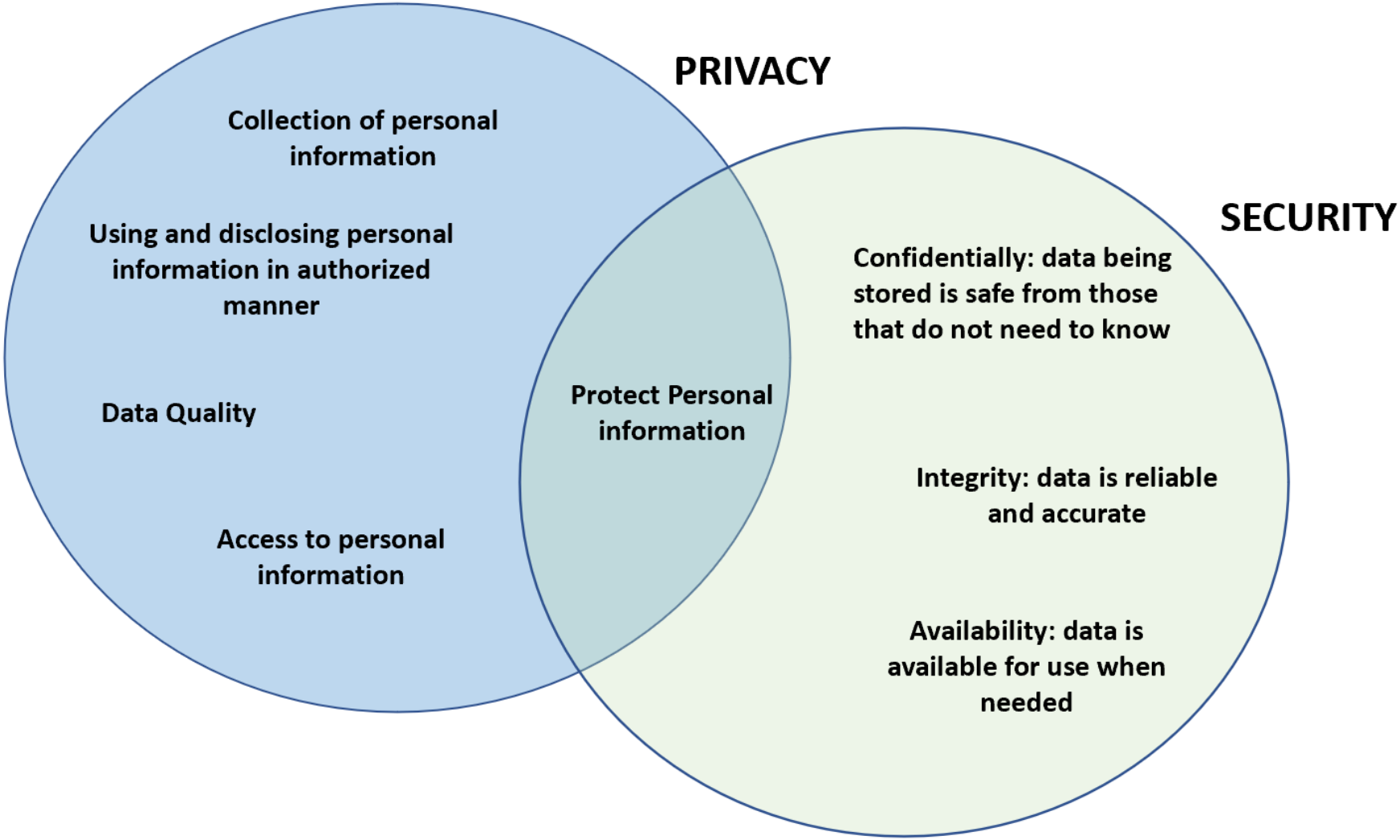
- When you think of computer security, think of Confidentiality, Integrity and Availability (aka CIA triad).
  - **C**onfidentiality: Limit access and disclosure to authorized users; those with a “need-to-know”.
  - **I**ntegrity: Limit the number of people, or processes that can modify information in the system.
  - **A**vailability: Maximize system uptime, and information availability to the right users.

Privacy

- Privacy is an individual's right to control the use and disclosure of their own personal information.
  - Individuals can assess a situation and determine how their data should be used.
- Privacy is the protection of customers or individuals and their personal information, for example, health and financial information.

Washington State Health Care Authority

Privacy and Security



Security Baseline Questions

- What is the purpose of this training?
  - CMS Compliance, Protecting Personal Identifiable Information (PII), Security & Privacy Awareness.
- Who is the weakest link in any security program?
  - People.
- Who is responsible for Security?
  - Everybody is!
- What information is critical for us to protect?
  - All information we receive, particularly, PII, Personal Health Information (PHI), Personal Care Information (PCI), and Federal Tax Information (FTI).

Security Baseline Questions (cont.)

- Where should you store electronic WAHBE Information?
  - Network Drives, OneDrive.
- With whom can you share critical WAHBE information?
  - Only people that need-to-know.
- With whom can you share your password with?
  - No one.
- Who would you contact if there is a Security incident to report?
  - Your HCA point of contact is hcavolunteerassister@hca.wa.gov.

Security Tips

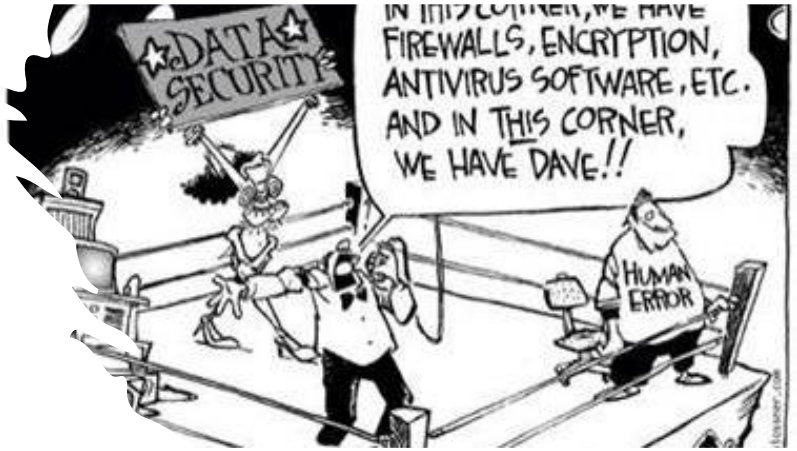
- Use secure network drives instead of local hard drives.
- Do not share your passwords or write them down.
- Do not post confidential or sensitive WAHBE information on any social networking site.
- Erase confidential information from whiteboards.
- Protect PII as if it were your own.
- Practice “need-to-know”.

Security Tips (cont.)

- Logout of systems before closing browser/windows.
- Protect your access cards, laptops and devices.
- Lock your computer.
- Use secure emails for sensitive information.
- Ensure that “role based” training is provided for everything you are given access to.
- Know who to contact in case of security questions/incidents.

Who is Responsible?

- HCA community partners who become a volunteer assister with access in Washington Healthplanfinder and users of Information Technology systems are equally responsible for security and privacy.
- No one is exempt.



Threats

Types of Threats

- Social Engineering
  - Phishing
  - Spear Phishing
  - Tailgating
  - Pretexting
  - Vishing
- Insider Threats
- Weak Passwords
- Misdirected/Unsecure Emails
- Oversharing Information

People are the weakest link in computer security!

Social Engineering

- Social engineering uses persuasion or influence to deceive personnel into divulging confidential information or allowing the adversary to perform unauthorized actions. Examples include:
  - Phishing – deceptive emails sent by bad actors, websites, and text messages that are used to steal information.
  - Spear Phishing – attack that targets specific individuals or groups within an organization.
  - Tailgating – when someone without proper authentication follows an authenticated employee into a restricted or protected area.

Opening Malicious Emails

- The impact of opening an attachment that is included in a malicious email can be very dangerous and expensive. The attachment may include a keylogger or install ransomware.
  - Keyloggers steal personal information such as usernames and passwords, take periodic screenshots, grab sent emails or harvest credit card numbers and bank details.
  - Ransomware is a type of malware attack that prevents or limits users from accessing their systems by locking the systems screen or the users file until the ransom is paid.

Insider Threats

- Too often, people associate the term “Insider Threats” in cybersecurity with malicious employees intending to directly harm the company through theft or sabotage. In truth, negligent employees or contractors unintentionally cause an equally high number of security breaches and leaks by accident.
- Insider threats is defined as an insider using their authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets.

Information

Personal Identifiable Information (PII)

- Per CMS, PII is anything that could individually, or in combination with other data elements, identify the consumer, such as a consumer's name, address, telephone number, social security number, Marketplace application ID or other identifier.
- Do not share client PII with others. Limit access and disclosure to authorized users; those with a 'need-to-know'.
- When in doubt contact your supervisor or your HCA Volunteer Assister point of contact.

Protected Information Collected

- Applicant/person's Information
  - Name, address, zip code, phone, DOB, SSN, ethnicity, etc.
- Household composition
  - Spouse
  - Children/dependents
  - Relationships
  - Medical conditions
  - Income information
- Username, email address, phone number
- Business/organization name
- Plan enrollment
- Enrollment history
- FPL%
- Citizenship status
- Incarceration status

Sources of Information

- Washington Healthplanfinder Portal (electronically)
- Paper Applications
- Federal Data Services Hub
  - SSA, DHS, DoD, VA, Peace Corps, CMS, etc.
- DSHS – Existing Medicaid population, ES Interface
- Letters and Correspondence
- Appeals
- Contracts and Agreements
- Issuers/Carriers
- Brokers, Navigators, IPAs, CACs, etc.
- Sponsorship Representatives
- Request for Washington Healthplanfinder user accounts

Unauthorized Disclosure Penalty

Per 45 CFR 155.260

- Improper use and disclosure of information (including PII):
  - Any person who knowingly and willfully uses or discloses information in violation of section 1411(g) of the Affordable Care Act will be subject to a civil penalty of not more than $25,000 per person or entity, per use or disclosure, in addition to other penalties that may be prescribed by law.

Unauthorized Disclosure Penalty

User Access Agreement

- The terms and conditions of this agreement will remain in effect after I leave my current position. I will not disclose confidential personal and financial information that I obtained while working in my position.
- I understand that any breach of any provision of this Agreement will subject me to disciplinary action, including the immediate termination of my access to Healthplanfinder, and termination of my position.

Prevention Tactics

Strong Password Characteristics

- Upper- and lower-case letters.
- A minimum of one special character.
- At least 15 alphanumeric characters long.
- Random passwords and pass phrases are the best defense in protecting sensitive information.

Tip: Create a passphrase, e.g. "This May Be 1 Way to Remember!" and the passphrase could be: "TmB1w2R!" or "Tmb1W>r!" or some other variation.

Sending Secure Emails

- Sending client PII via emails should be avoided.
- If necessary, PII must be sent via encrypted emails only. Before sending such emails, verify recipients are:
  - Authorized to receive such PII; and
  - Need-to-know.
- Avoid sending PII but, if necessary, encrypt it.
  - You will need to engage your own IT resource for assistance with an encryption process that works with your email system.

Incident

Incident

- Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail or email, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

Breach

- An incident becomes a breach when there is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for another than authorized purpose have access or potential access to PII or Federal Tax Information (FTI) whether physical or electronic.

Common Vulnerabilities

- Casual handling of confidential information (electronic, hardcopies).
- Loss or theft of laptop/device.
- When including screenshots, make sure that no PII or FTI is visible.
- Too much access (least privilege not followed).
- Losing employee access badges.
- Non-compliance with policies, procedures, standards and regulations.
- Tailgating.

Common Vulnerabilities (cont.)

- Unauthorized or unintended disclosure of PII, or FTI, when sending unsecure emails or including too much information in Help Desk tickets.
- There is no need to put any client information found from other sources (phone number, address, etc.) Minimize putting PII in tickets by:
  - Describing the problem, not the people.
  - Using Anonymous data such as the Application ID or Person ID.
    - Do not put SSN's (not even the last 4).
  - Never post any kind of user or individual lists in tickets.

How to Prevent an Incident

- Only discuss confidential information with those who have a 'need-to-know'.
- Documents containing confidential information should never be left out in the open. Tips to prevent this, include:
  - Discard in labeled/locked shredder bins.
  - Lock your computer screens.
  - Do not leave it exposed in your work area, and
  - Always use secure print.
- Avoid emailing sensitive information.
- Follow physical and information security policy, standards, procedures and guidelines, at all times.
- When in doubt, consult the WAHBE Security Team security@wahbexchange.org.

Publicly Accessible Info

- All shared materials must not contain confidential content (PII, IT system settings, consumer-specific information, etc.).
- Do not post company specific information, consumer specific information, or PII on social media.

For more information visit: https://www.wahbexchange.org/new-customers/application-quick-tips/privacy-tips/

Security Incidents – Your Role

- If you see something, say something.
- If you become aware of an incident, contact WAHBE Security immediately at security@wahbexchange.org.
  - Assisters be sure to also copy your lead org.

Tip: Please do not directly contact the Center for Medicare & Medicaid Services (CMS) or the Internal Revenue Service (IRS) yourself!

Volunteer Assister Access

Volunteer Assister Access in Washington Healthplanfinder

- Be affiliated with an organization and complete all 7 modules of the Community-Based training.
- Request a training assessment test at hcavolunteerassister@hca.wa.gov.
- Complete and return the test to the same email address.
  - Upon successful completion of the test, HCA will email the Volunteer Access Registration Packet: Community Partner Registration Form, WA State Background Check, and Washington Health Benefit Exchange User Agreement.
- Once approved, you will be granted volunteer access in Washington Healthplanfinder and emailed a personal username and password.

Washington Healthplanfinder Account Reminders

- If there has been no activity on your Washington Healthplanfinder account in 180 days your access will be disabled.
- Passwords for Washington Healthplanfinder expire every 60 days.

Resources

- HCA Training & Education
  - hca.wa.gov/free-or-low-cost-health-care/i-need-medical-dental-or-vision-care/training-and-education-overview
- HCA Area Representatives
  - hca.wa.gov/assets/free-or-low-cost/area_representatives.pdf
- Contact Us
  - hcavolunteerassister@hca.wa.gov
- WA Health Benefit Exchange
  - wahbexchange.org/

Congratulations!

- You have completed the full 7 module HCA Community Based Training!
- Please contact HCA at hcavolunteerassister@hca.wa.gov for the final steps to test and apply for volunteer assister access in Washington Healthplanfinder.

Washington State Health Care Authority