# SECURITY AND PRIVACY AWARENESS

## WAHBE Security Team

washington
healthplanfinder
powered by the Washington Health Benefit Exchange

# PURPOSE

01 To provide training on Security and Privacy topics

02 To establish a baseline of HBE Security

03 To increase Security and Privacy Awareness

04 For CMS and IRS compliance

# WHAT IS PERSONAL IDENTIFIABLE INFORMATION?

## Commonly referred to as PII

01 Per the Department of Labor, PII is *"Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."*

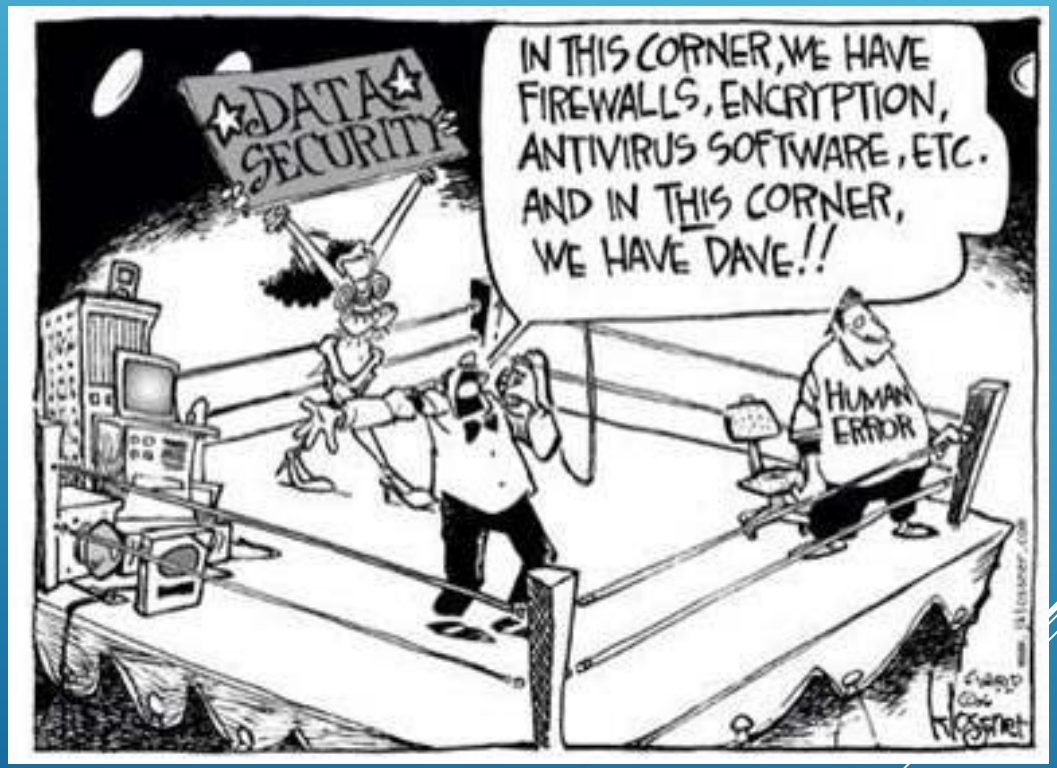
02 Any single piece of info or info that can be used in conjunction to ID an individual

03 Do not share client PII with others. Limit access and disclosure to authorized users; those with a "need-to-know".

04 When in doubt contact your supervisor, lead organization or the Washington Health Benefit security team (security@wahbexchange.org).

# WHO IS RESPONSIBLE?

- Everyone is equally responsible for Security and Privacy, no one is exempt




Proprietary & Confidential

# SECURITY

When you think of computer security, think of Confidentiality, Integrity and Availability (aka CIA triad)

CONFIDENTIALITY: Limit access and disclosure to authorized users; those with a "need-to-know"

INTEGRITY: Limit the number of persons who can modify information in the system

AVAILABILITY: Maximize system uptime, and information availability to the right users

Proprietary & Confidential

# COMMON WAHBE VULNERABILITIES

- Casual handling of confidential data
- Loss or theft of laptop/device, softcopy/hardcopy data
- Unauthorized or unintended disclosure of PII
  - Sending unsecure emails
  - Including PII in IT helpdesk tickets
  - Not using secure print
  - While being helped, or helping others
  - Sharing information with co-workers that falls outside of the role of the navigator
- Too much access (Least Privilege not followed)
- Losing employee access badges
- Conflicts of interest
- Lack of oversight

This Photo by Unknown Author is licensed under CC BY-SA

# TYPES OF WAHBE THREATS

- Social Engineering
  - Phishing
  - Shoulder surfing
- Insider Threats (e.g., Running unauthorized software, scripts, etc.)
- Weak Passwords
- Poor Internet Hygiene
- Malware
- Unauthorized Access to System
- Misdirected/Unsecure Emails
- Oversharing Information
- Tailgating

# POLL

You often meet clients at a local coffee shop for appointments. During your appointment today at the coffee shop you are going to help a client create an account and select a QHP. What can you do to protect your clients PII while still working in a sometimes-crowded public area?

This Photo by Unknown Author is licensed under CC BY-SA



Proprietary & Confidential

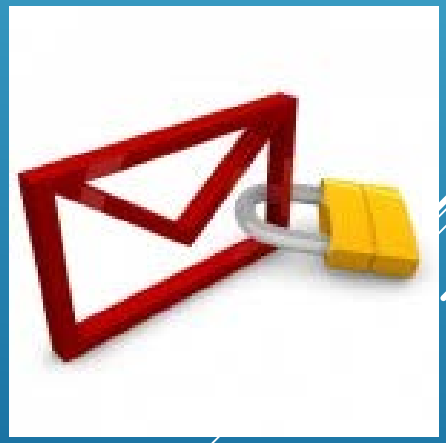
# STRONG PASSWORDS CHARACTERISTICS

- Upper and lower case letters
- A minimum of one special character
- At least eight alphanumeric characters long
- **14 Characters is the optimal password length** (example will be provided)
- **Pro Tip:** Try to create passwords that can be easily remembered, e.g., "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation

This Photo by Unknown Author is licensed under CC BY-NC

# 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
    - Verify recipients need-to-know
- To encrypt use one of the following the beginning or the end of the subject line:
  - \S
  - \E
  - **secure**
  - **encrypt**



This Photo by Unknown Author is licensed under CC BY-SA

# PROTECTED INFORMATION

## INFORMATION WE COLLECT

- Applicant/User Information
  - Name, Address, Zip code, Phone, DOB, SSN, FTI, Ethnicity, etc.
- Household Composition
  - Spouse
  - Children/Dependents
  - Relationships
  - Medical Conditions
  - Income Information
  - Federal Taxpayer Information (FTI)
- Business/Organization Name
- HPF Business Employer & Employees' details
- Plan Enrollment
- Enrollment History
- Federal Poverty Level (FPL) %
- Citizenship Status
- Incarceration Status, etc.

## SOURCE OF INFORMATION

- 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 Healthplanfinder user accounts
- Employment Applications
- WAHBE Office space
- WAHBE Business Dealings, etc.

This Photo by Unknown Author is licensed under CC BY-SA

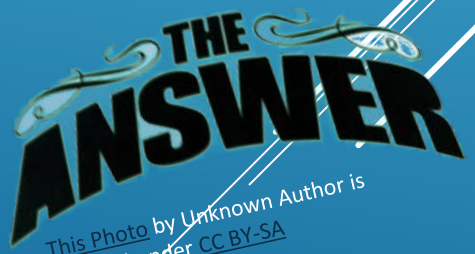
# SCENARIO 1

What if a patient expects us to know about their plan, because we enrolled them, so they do not bring their insurance card to their doctor appointment? If I'm asked by someone in my organization about an enrollee's coverage, like someone in the billing department or a nurse or doctor, can I look up the information in Healthplanfinder and answer their question?

# SCENARIO 1 CONTINUED

No!

1. The navigator regulations and user agreement state a navigator may only share information with others as needed to perform Exchange/navigator functions. Confirming coverage for billing or scheduling purposes is not a navigator function.
2. The consent documented by the navigator in Healthplanfinder gives permission to access personal, confidential information only to the navigator – not to any others.




This Photo by Unknown Author is licensed under CC BY-SA

# POLL

All the producers/navigators in your office have gone on vacation and you are the only one in the office for the next week. You receive a call from a client of one of the producers/navigators on vacation.

The client wants you to upload a document to prove they are not incarcerated. You explain that you can work on behalf of their agent/navigator since they are on vacation. The client emails you the document needed, and you successfully upload it into their account.

Later you receive a call from one of your clients asking what documents are needed to prove they are not incarcerated. You remember that you just uploaded proof of non-incarceration documents into another account.

Can I access my colleague's client's account to look at what documents were used to prove they were not incarcerated?

# SCENARIO 2

Following is a situation as described by a navigator:

We had a couple on one application, meaning we have permission to talk to both of them about the information in that application. The husband came to update the application, and a few weeks later, the wife came and told us they had actually been separated due to domestic violence.

Only because they saw the same navigator did we put together that we had worked with the husband, and that she wanted to take him off the application. If he came back and asked us why, without the same navigator knowing the situation, we would have given the husband information about the wife that we shouldn't have because of domestic violence.

For more information refer to the Application Permissions Matrix located in the Troubleshooting Desk Aid located on your LMS dashboard

Proprietary & Confidential

# SCENARIO 2 CONTINUED

Regarding the first paragraph, consider…

1. Who is the primary applicant (PA)?
2. Is the spouse listed as an authorized representative on the application?
   - The PA is the only person that can authorize any change to an application, unless there is a designated authorized representative.
   - You should always refer to the Application Permission Matrix found in your Troubleshooting Desk Aid for these types of situations.

Please refer to the Domestic Violence section of the Troubleshooting Desk Aid step-by-step directions in working with a survivor of domestic violence.

This Photo by Unknown Author is licensed under CC BY-SA

# SCENARIO 2 CONTINUED

Paragraph 2: "Only because they saw the same navigator did we put together that we had worked with the husband, and that she wanted to take him off the application. If he came back and asked us why, without the same navigator knowing the situation, we would have given the husband information about the wife that we shouldn't have because of domestic violence."

Assuming she is the PA and took the appropriate steps to remove her spouse from her application, they would now be under separate accounts and separate applications and no information should be disclosed about her to the spouse. As a navigator you should explain that since this couple is no longer on the same application you are not authorized to provide any information about either individual to the other.

This Photo by Unknown Author is licensed under CC BY-SA

# SCENARIO 3

My assister organization provides other services, such as health care or social services, that are separate and apart from my duties as an Assister (navigator/CAC). If an assister organization would like to obtain a consumer's consent to create, collect, disclose, access, maintain, store, or use their PII for purposes other than what is in the scope of their regular assister duties, is this permitted?

# SCENARIO 3 CONTINUED

To protect the navigator and the organization, the patient would need to give separate consent for their information to be used for another purpose. The consent would need to document the purpose of the disclosure and would need to be saved. You would need to be able to demonstrate that the patient gave permission to use PII in Healthplanfinder for another purpose. As long as this additional consent is used, the navigator and their organization will be covered.

This Photo by Unknown Author is licensed under CC BY-SA

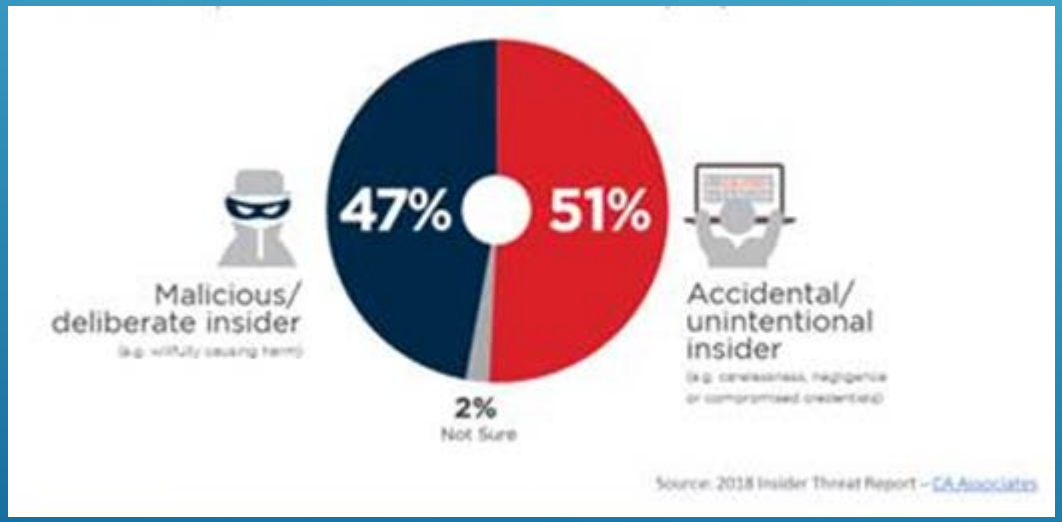
# LOSS OF MOBILE DEVICES

If a device that contains or may potentially contain PII is misplaced, or the device owner/user loses the control of the device for an extended duration, you must immediately report it to your supervisor, WAHBE IT Security (security@wahbexchange.org) and copy navigator@wahbexchange.org with the details, such as,

- Date, time, and place of loss
- Nature of loss
- Circumstances leading to the loss
- Date and time law enforcement authorities informed
- Outcome of such contact
- Your follow-up activities, etc.

# 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.



# 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.

# INCIDENT

Violating an explicit or implied security policy, which includes these attempts

This Photo by Unknown Author is licensed under CC BY-SA

### Item 01

Gain unauthorized access to a system or its data

### Item 02

Execute unwanted disruption or denial of service

### Item 03

Obtain unauthorized use of a system for the processing or storage of data

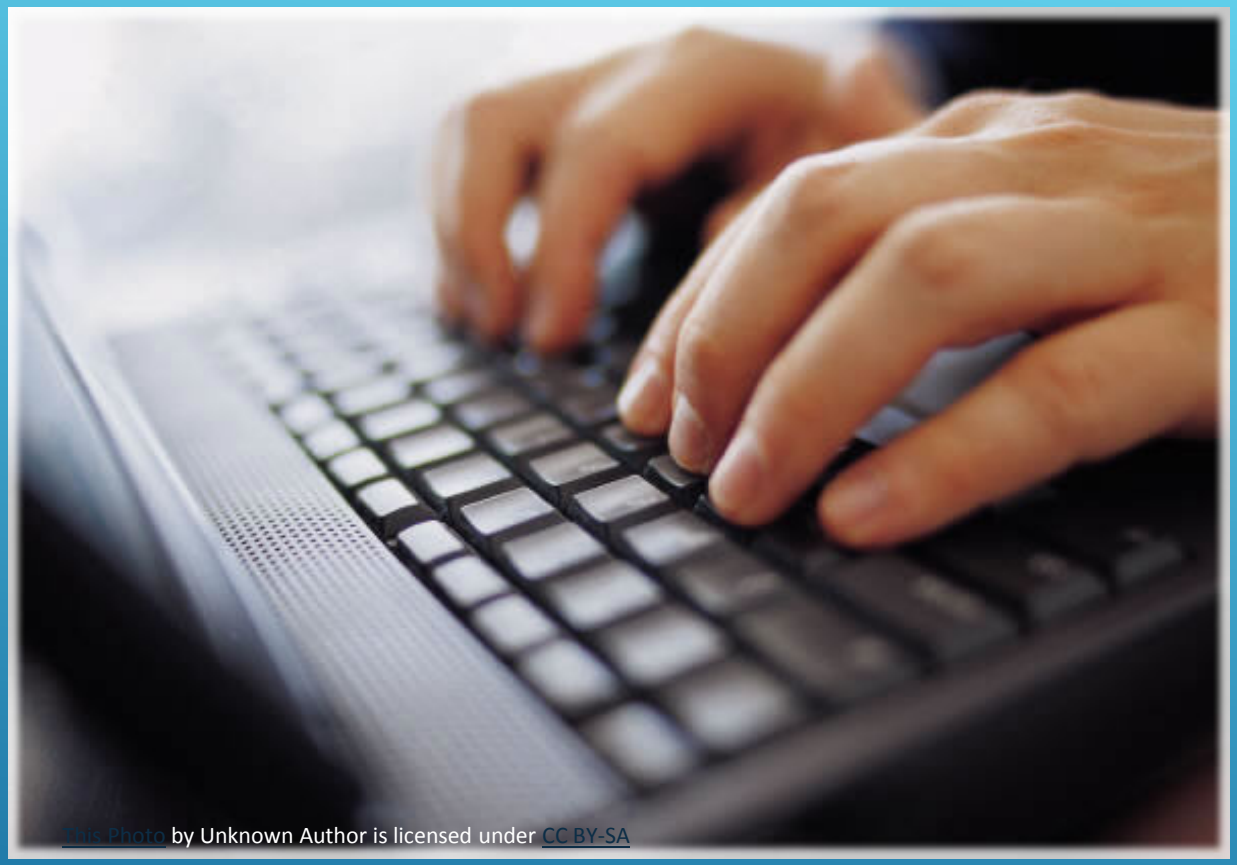
### Item 04

Make changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

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

This Photo by Unknown Author is licensed under CC BY-SA

# SECURITY INCIDENTS- YOUR ROLE

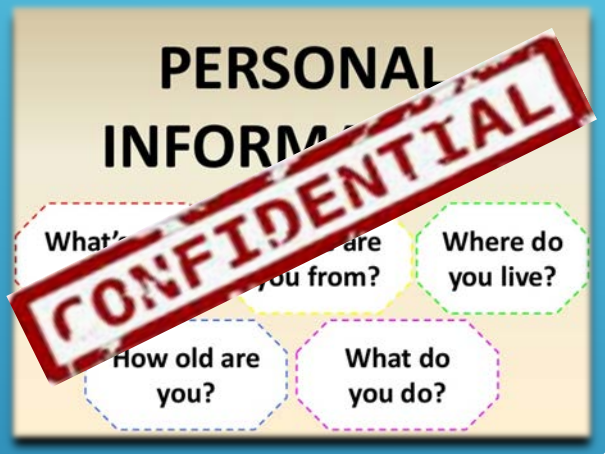



Email: security@wahbexchange.org and copy navigator@wahbexchange.org or producersupport@wahbexchange.org

- *Please do not directly contact CMS or IRS yourself!*

# HOW TO PREVENT AN INCIDENT

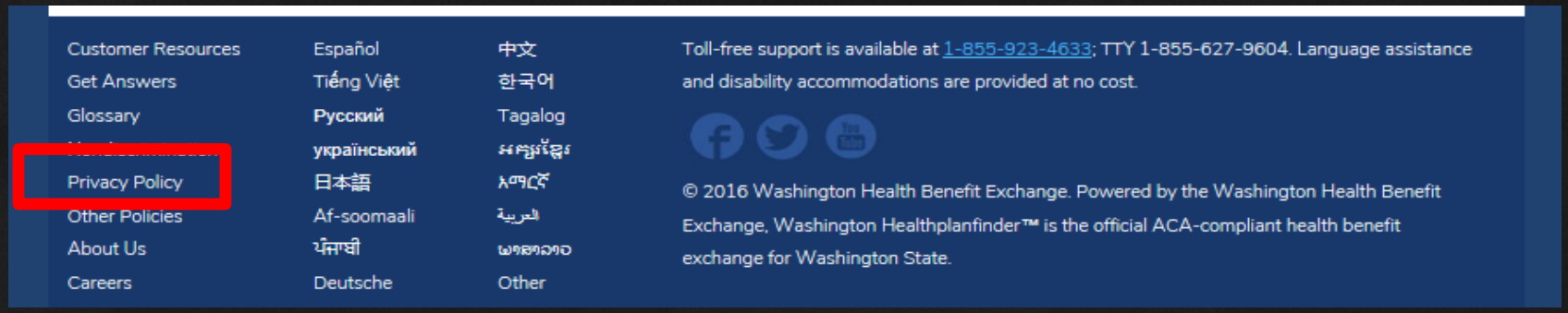
- Only discuss confidential information with those who have a "need-to-know"
- Documents containing confidential information should never be left out in the open:
  - Discard in labeled/locked shredder bins
  - Lock your computer screens
  - Don't leave it exposed in your work area
  - Always use secure 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




This Photo by Unknown Author is licensed under CC BY-NC-ND

# WAHBE Privacy Policy Highlights

1. PII is used only for authorized purposes.
2. PII is not disclosed to unauthorized third parties.
3. Only anonymous info may be shared with third parties.
4. We protect the confidentiality of Individual's PII.
5. We perform ID Verification to protect privacy.
6. We continue to evaluate our efforts to protect PII.
7. We will provide notice of changes in our information privacy practices.
8. We will notify individuals in case of PII use changes and individuals will have a choice to opt-out.


Customer Resources
Get Answers
Glossary
Privacy Policy
Other Policies
About Us
Careers
Español
Tiếng Việt
Русский
український
日本語
Af-soomaali
ਪੰਜਾਬੀ
Deutsche
中文
한국어
Tagalog
ᨅᨔᨕᨘᨁᨗᨔᨕᨁᨗᨔᨕᨁᨗᨔᨕ

# User Access Agreement

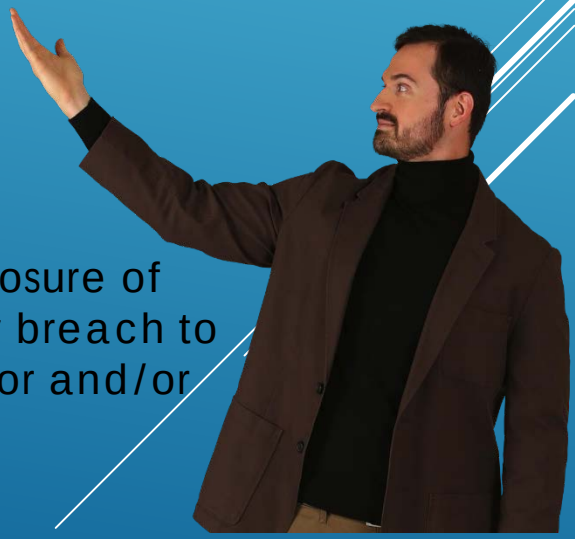
1. I will only create, collect, use, or disclose confidential personal and financial information to the extent it is necessary to carry out my authorized role with the Exchange, and for no other purpose.

2. I will disclose confidential person and financial information only to individuals who are authorized to receive or view it. If I receive any request for information from an unauthorized person or uncertain entity, I will promptly refer the request to the Navigator/Broker team at the Exchange, to my supervisor and/or Lead Organization.

3. I will not disclose my password or any other account information to anyone, and will not allow anyone else to use or have access to my Healthplanfinder Account.

4. I will not use my account in a manner that is illegal, that could lead to disruption of the Healthplanfinder services, or that could pose a risk to the security of the Healthplanfinder.

5. I will immediately report any unauthorized access or disclosure of confidential personal and financial data. I will report any breach to the Healthplanfinder Navigator/Broker team, my supervisor and/or Lead Organization.



# User Access Agreement

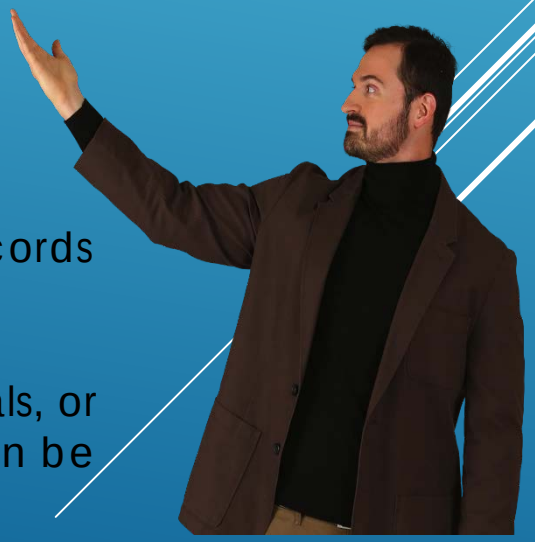
6 I have received a copy of and read the Exchange's privacy policy, and have received training on the Exchange's privacy and security standards.

7 I will comply with all policies and procedures of the Exchange regarding privacy and security of confidential and personal information in accordance with 45 CFR 155.260. I understand that any violations of the nondisclosure of confidential and personal information requirements may subject me to civil fines up to $25,000 per use or disclosure.

8 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.

9 I understand that any breach of any provision of the Agreement will subject me to immediate termination of my access to the Healthplanfinder.

10 I will be given access to information submitted to and records stored by the Washington Health Benefit Exchange. That information includes confidential personal and financial information gathered from applicants, qualified individuals, or enrollees through the Healthplanfinder webpage that can be used only for Exchange business purpose.



# AUTHORIZED PURPOSE

I will only create, collect, use, or disclose confidential personal and financial information to the extent it is necessary to carry out my authorized role with the Exchange, and for no other purpose.

01 Input data in Healthplanfinder to assist a customer to obtain Health Insurance.

02 Change Reporting to keep client's account up to date and eligibility current.

03 Accessing your customer's account without their knowledge and permission for any reason is a violation of this agreement.

04 Having unauthorized access to information to any customer's confidential personal and/or financial data must be reported. It is a violation of this agreement to use that information for any purpose.

# PUBLICLY ACCESSIBLE INFO

- Reviewed before posting, sharing or releasing.
- All shared material must *not contain* confidential content (PII, system settings etc.)
- *Do not post company specific information or PII on social media*.

This Photo by Unknown Author is licensed under CC BY-NC

# Create a Help Ticket

- **Describe the problem, not the person**
- **Do not enter PII in IT help tickets:**
- **Do no put SSN's (not even the last 4)**
- **There is no need to put any client info that we can find from other sources (phone number, address, etc.)**
- **Use Anonymous data instead (Application ID, Person ID, etc.)**
- *Never post any kind of user or individual information in tickets*
- **When including screenshots, make sure that no PII is visible**

# POLL

Your long-time client will be experienced an involuntary loss of MEC, their employer sponsored coverage is ending soon. You completed an application with your client. You realized when you received the coverage effective date, that your client's new coverage will not start next month, but the following month. When you reviewed the application, you realize you input the wrong date of loss for their group coverage.

You are preparing an email for Producer Support (or contacting your Lead Organization) to create a ticket so your client's effective date will be next month to prevent a gap in coverage. Your client has many serious medical needs that must be addressed. They must be seen by their PCP next month to treat their diabetes, hypertension and heart conditions. They also have several prescriptions that need to be filled. In your email, should you explain your client's medical needs in detail to ensure your email is a priority?



Proprietary & Confidential

# SECURITY TIPS

This Photo by Unknown Author is licensed under CC BY-ND

- 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
- Practice "need-to-know"
- Logout of systems before closing browser/windows
- Protect your access cards, laptops and devices
- Watch for tailgaters (ask them to swipe those badges)
- 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

# POLL

You have been locked out of your HPF account. You have important client meetings all morning and you don‘t have time to send an email to Producer Support or Navigator LMS to unlock your account.  These are important meetings and you have to have access to your HPF account for your client meetings.
To save time can I have my Admin Assistant or co-worker send an email to my support at WAHBE to unlock my account?  Since my admin/co-worker has access to my email and voice mail so I can work more effectively this shouldn’t be a problem.  They also have access to my HPF account to service my clients’, so will be able to make sure my HPF account is unlocked.

# SECURITY BASELINE QUESTIONS

- What is the purpose of this training?
  - ✓ CMS Compliance, Protecting PII, Security & Privacy Awareness
- Who is the weakest link in any security program?
  - ✓ Human Element/People
- Who is responsible for the Security at WAHBE?
  - ✓ Everybody!
- What information is critical for us to protect?
  - ✓ All Information we receive, particularly, PII, PHI, PCI, and FTI
- 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 supervisor, Security team, or send an email to security@wahbexchange.org and copy navigator@wahbexchange.org or producersupport@wahbexchange.org

# Password Strength Demo

www.grc.com/haystack.htm

# RESOURCES

Report a Breach, Incident, have a question regarding Security security@wahbexchange.org and copy either your producer support team or your navigator team.

- Brokers – producersupport@wahbexchange.org
- Navigators - navigator@wahbexchange.org
- Tribal Assister - navigator@wahbexchange.org
- Certified Application Counselor - navigator@wahbexchange.org

1. **HPF Account Lockout support**
2. **HPF Application Support**
   - Brokers – producersupport@wahbexchange.org
   - Navigators - navigator.lms@wahbexchange.org
   - Tribal Assister - navigator.lms@wahbexchange.org
   - Certified Application Counselor – navigator.lms@wahbexchange.org



Proprietary & Confidential