Aged and Disabled Waiver- Provider Privacy Guide

Introduction:

The Aged and Disabled Waiver Provider Privacy Guide is a resource guide that identifies reputable sources for privacy information. This guide is not intended to cover all privacy information and is intended to be used solely as a resource for locating valuable educational information. Your specific provider agency may have specific requirements that are not included in this guide. Remember to always check your provider agency policies and procedures or your agency's privacy official.

Privacy Tips

- Do not place a member's name, Medicaid number or other identifying information in the subject line of the email
- Do not include sensitive medical information such as member diagnoses or health conditions in unsecure emails (emails that are not encrypted)
- Do not use member's name or other identifying information in a text message (may use initials)
- Agency cell phones must be encrypted for security
- Do not discuss a member's personal information in hallways, in public places, with other members or your personal home(need to know basis)
- Always utilize encrypted emails when including identifying member information such as member name, Medicaid number, or other identifying information
- Ensure that laptops, computers, phones, IPad's or other electronic devices are password protected and encrypted if at all possible
- Keep member records or electronic devices containing member identifying information stored in a safe and secure location (not the trunk of your car)
- Refrain from use of personal electronics when including member information
- Password protect business electronics such as phones, laptops or IPad's
- Ensure that the fax machine that you are sending or receiving is a secure fax machine
- Ensure that emails and electronic devices are encrypted
- Ensure that no one shares a password on a computer, cell phone or other electronic device
- Ensure computer monitor is not facing a window or the public
- Lock your computer OR your door when leaving your desk to prevent access to personal information
- Use a cross cut shredder to destroy paper documents
- For shredding companies, ensure that there is a privacy agreement (company may transport documents to another location for shredding)
- For storage of files in a remote location, and sure that there is a privacy agreement
- Before discarding computers, phones, fax machines, copiers, iPad, scanners or other electronic devices, ensure that the memory is clean
- Do not store member personal information on a personal device such as a personal computer, personal cell phone, personal iPad

Managing Privacy Effectively

Question:

What can I do to protect personally identifiable information (PII), such as credit card numbers, Social Security Numbers, and driver's license numbers?

Answer:

Privacy is a big job. All employees could possibly access PII – about both co-workers and citizens. Everyone has to work hard to protect that PII at all times.

The privacy policies and procedures provide the rules for using and sharing PII. But some common sense can help you avoid common problems.

1. **Be organized.** PII is contained in so many documents, and on almost every computer and storage device. To help prevent losses, keep careful track of documents and storage media. If something does get lost, you'll also realize it sooner and be able to react quickly.
2. **Be careful**. Most security breaches happen because of a simple mistake. For example, it's very easy to put the wrong address on a label, or the wrong label on a package. Double check the address and phone numbers when faxing.
3. **Be skeptical.** Don't be afraid to ask questions if someone asks you to use or share PII in a new way. If someone tells you they've deleted the PII from a shared flash drive, check it before you toss the drive in your pocket.
4. **Be honest.** Everyone makes mistakes. If you make a mistake with PII, or if you've misplaced PII, contact your supervisor. They can work with your department's privacy officer to recover the PII and address any possible harm.
5. **Learn from the mistakes.** Everyone makes mistakes, but if we make the same mistakes over again, it shows that we're not learning. If you have a problem with a certain process, your supervisor or privacy officer can help you find a way to minimize the likelihood of repeated incidents.

Resources

WV State Privacy Office:

Website link: http://www.privacy.wv.gov/Pages/default.aspx

The West Virginia Executive Branch Privacy Program balances an individual's right of privacy against others' need and right of access to PII. The Privacy Program is based upon these six Privacy Principles, consistent with law and policy:

- Accountability
- Consent
- Individual Rights
- Minimum Necessary and Limited Use
- Notice
- Security Safeguards

Information is available on this website that addresses each of these areas. Examples of policies, business agreements, etc. are available as a resource. Please keep in mind this information addresses current policies and procedures for the state of WV and will not be specific to your provider agency.

US Department of Civil Rights: (HIPAA)

This website includes information regarding federal information on HIPAA, training materials, patient privacy, information technology, disaster response, complaints, the sample associate business contract, summary of security role frequently asked questions, etc. Please keep in mind this information addresses current federal and will not be specific to your provider agency.

http://www.hhs.gov/ocr/privacy/index.html

Bureau of Senior Services: HIPAA and Privacy Tips

This website link includes posts of WV state government HIPAA and privacy tips that were distributed to state employees. Please keep in mind this information addresses WV state government and will not be specific to your provider agency.

http://www.wvseniorservices.gov/StayingSafe/HIPAAPrivacyTips/tabid/149/Default.aspx