

West Virginia Executive Branch Privacy Policy: Accountability

Everyone is Responsible for Protecting PII

QUESTION:

Am I responsible for protecting PII?

ANSWER:

Each Department must protect personally identifiable information (PII). Each Department must also comply with privacy laws. The Privacy Office has developed policies and procedures to protect PII, but everyone in the Department must work together to achieve our privacy and security goals.

Here's what you can do:

- ✓ Read and understand your confidentiality agreement.
- ✓ Take the privacy training courses.
- ✓ Follow all the policies and procedures that apply to your job and activities.
- ✓ Ask questions if you aren't sure about how to comply with the policies and procedures.
- ✓ Use the resources that your privacy officer makes available.
- ✓ Tell your privacy officer about privacy complaints or security concerns.
- ✓ Report any mistakes that accidentally expose PII immediately.

Our privacy program empowers you to make good decisions about PII. If you are ever asked to use or share PII in a way that isn't consistent with the privacy policies, you must say no!

Tip 2: Making the Most of Your Privacy Training

You should have completed training as part of your orientation. You may have received additional privacy training as well.

Taking training courses is part of everyone's job, but here's how to make the most of your privacy training experiences:

- ✓ Give the training course your full attention. We all struggle with competing work demands, but it's best to focus on the training completely. Leave your blackberry and other work behind. You'll learn more, and it will be more interesting!
- ✓ Think about how the material covered in the training applies to the PII you handle. Are you comfortable that you understand all the rules? If not, ask your privacy officer for additional guidance.
- ✓ Give your privacy officer honest feedback on the training. Was it too easy or too hard? Did it provide you with information that you found helpful? Your privacy officer welcomes suggestions for how to making the training more useful.
- ✓ If there are other areas that you think the training should cover, be sure to share that with your privacy officer too.

Tip 3: Privacy or Security Questions? Get Answers!

Everyone has questions about privacy and security from time to time. Your privacy officer has the resources you need to get answers! Did you know:

- ✓ Your privacy officer welcomes questions!
- ✓ Your privacy officer can help you understand privacy and security rules for any particular situation. New assignment? New PII? Your privacy officer can tell you what you need to know.
- ✓ You also have access to a website full of privacy tips and other information. Visit **West Virginia's Online Privacy Office** at <http://www.wvprivacy.org/> to see what's available.
- ✓ The Online Privacy Office has tips to help you protect your own privacy. The website includes information on identity theft and credit reports.
- ✓ You can also find copies of all the policies and procedures at the Online Privacy Office.

Tip 4: Understanding Your Confidentiality Agreement

Your Department is required to have all workers and vendors sign confidentiality agreements every year. Take a few moments today to think about what this agreement means for you.

- ✓ The confidentiality agreement is your promise that you will protect all the PII and other information entrusted to you by your Department.
- ✓ The agreement is your promise that you will use and disclose the PII and other Department information only as needed to perform your job functions.
- ✓ The agreement is legally-binding, just like other contracts you have signed. This means that the Department can use the courts to enforce the agreement, should you violate it.
- ✓ The agreement protects you too, by ensuring that your own PII is handled properly by others in the Department. For example, everyone that handles your payroll information is bound by these terms as well.
- ✓ Making every worker sign a confidentiality agreement is a reflection of the Department's commitment to protect the privacy of its workers, vendors and citizens. Keeping the promises you made when you signed the agreement is how you do your part!

If you have any questions about your confidentiality agreement, or if you need another copy for your files, please contact your privacy officer or human resources manager.

Tip 5: Managing Privacy Policy Violations

Following the privacy and security policies is the right thing to do, but it's also a condition of your job. Workers who violate the policies and procedures may be subject to disciplinary action, and serious or repeat violations may result in termination of your employment or contract.

Here are some steps to take to reduce the likelihood that you will wind up in trouble:

- ✓ Understand all policies and procedures that apply to your handling of PII.
- ✓ Be cautious when you are asked to use or disclose PII in a new or different manner. It's always OK to ask questions if you aren't sure about the right thing to do.
- ✓ Recognize that PII in transit is always PII at risk. Be extra careful when sending PII to other people, such as via email. Double check the address.
- ✓ Never download PII to an unapproved device or storage media.

Even with your best efforts, however, understand that you may still make a mistake. Your privacy officer understands this! Immediately report any inappropriate uses or disclosures of PII to your privacy officer. This way the Department can take steps to minimize the harm – and the consequences!

Tip 6: Handling Privacy Questions and Complaints

Do you know what to do if someone complains about how PII is being used?

- ✓ Everyone has a right to understand the Department's privacy and security practices. This is true for department workers, consumers, citizens and suppliers.
- ✓ The Department's Privacy Notice can be found online at West Virginia's Online Privacy Office. See <http://www.wvprivacy.org/>. Many privacy questions can be answered by reading this Notice.
- ✓ If the Privacy Notice doesn't provide the answer, contact your privacy officer.
- ✓ If a person believes that his or her PII is being used inappropriately, that person has a right to complain. **Never discourage a person from asking a question or making a complaint.**
- ✓ You should refer all privacy and security complaints to your privacy officer immediately. Your privacy officer will investigate and respond to the individual directly.

Tip 7: Mistakes Happen – Responding to Privacy and Security Incidents

Even the very best privacy programs have incidents. People make mistakes and PII becomes exposed. The best privacy programs prepare for incidents. Workers know how to report mistakes. And privacy officers know how to respond.

All workers immediately must report all unauthorized uses or disclosures of PII to the privacy officer. This includes unauthorized internal disclosures. You should also report any other incidents that could expose PII. For example, the following types of events must be reported immediately:

- ✓ Lost or stolen laptops or devices (such as a PDA or cell phone),
- ✓ Lost or stolen storage media (such as a flash drive/memory stick or CD-ROM),
- ✓ Lost or stolen paper records containing PII,
- ✓ Accidentally sending PII to the wrong person (such as sending an email to the wrong address)
- ✓ Learning that PII was delivered to the wrong person by the postal service or courier,
- ✓ Accidentally sending PII in an insecure format, such as transmitting sensitive PII over the Internet in an unencrypted format,
- ✓ Lost or compromised passwords or access cards,
- ✓ Inappropriate up- or downloading of content (which could contain malicious code),
- ✓ Presence of viruses, spyware or other malicious code on a Department computer, or
- ✓ Any event that corrupts PII in a Department system.

If you become aware of any known or suspected misuse or improper disclosure of PII, you must also immediately notify the privacy officer.

Tip 8: Privacy and Security Breach Notification

If a security breach exposes PII, you must contact your privacy officer immediately.

Your privacy officer will decide whether to notify the individuals whose information was exposed. Your privacy office will notify individuals if there is a legal obligation to do so. Individuals will also be notified if they are at real risk of harm as a result of the breach.

If notification is needed, your privacy officer will decide how to provide notice and what the notice should say. For example, the notice will need to describe the incident. It will also tell the individuals what steps they need to take to protect themselves from harm.

It is very important to let your privacy officer handle breach notifications. This ensures that individuals receive the accurate and helpful information. Never attempt to notify individuals about a breach without the approval of your privacy officer!

Tip 9: Managing Privacy Effectively

Privacy is a big job. Everyone in the Department has access to PII – about both co-workers and citizens. And 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.

- ✓ **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.
- ✓ **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. When you're sending PII to another person, double check the address!
- ✓ **Be skeptical.** Don't be afraid to question other people, even managers. If someone asks you to use or share PII in a new way, make sure that it's okay. If someone tells you they've deleted the PII from a shared flash drive, confirm that before you toss the drive in your pocket.
- ✓ **Be honest.** Everyone makes mistakes. If you make a mistake with PII, or if you've misplaced PII, call your privacy officer immediately. The privacy officer can help you recover the PII and address any possible harm.
- ✓ **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 manager or privacy officer can help you find a way to minimize the likelihood of repeated incidents.