

West Virginia Executive Branch Privacy Policy: Accountability

Mistakes Happen – Responding to Privacy and Security Incidents

Question:

What are my responsibilities when a privacy or security incident has occurred?

Answer:

Even the very best privacy programs have incidents. People make mistakes and private information, (PI), 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 private information, (PI), to the privacy officer. This includes unauthorized internal disclosures. You should also report any other incidents that could expose PI. 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 PI,
- ✓ Accidentally sending PI to the wrong person (such as sending an email to the wrong address)
- ✓ Learning that PI was delivered to the wrong person by the postal service or courier,
- ✓ Accidentally sending PI in an insecure format, such as transmitting sensitive PI 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 PI in a Department system.

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