

West Virginia Executive Branch Privacy Tip of the Week

Data Destruction

Question:

Okay, so I work in a field office and we only have access to a couple of shredders - most of the time they're jammed. A few times when I couldn't use a shredder, I just ripped the old records (with names and social security numbers) into a few pieces and put them in the trash. Isn't that safe enough?

Answer:

Data can exist in electronic and paper formats. Do you know how to properly destroy data when it is no longer needed? Personally identifiable information (PII), such as social security numbers, employees' home addresses, and driver's license numbers, can be exposed or compromised from old records, so it is critical to ensure that the records are destroyed appropriately to prevent unauthorized disclosure and use.

Here are some steps you can take to ensure PII is properly destroyed:

- ✓ Know and follow any data retention policies established by your department. These policies generally establish the length of time documents of various types must be kept.
- ✓ When data has reached its end of life, follow established procedures for securely destroying that data. For paper documents, shredding is the most common form of destruction. For electronic documents, multiple rounds of data overwriting-are often used. Alternatively, the media should be physically destroyed.
- ✓ Be sure to consider destruction of electronic records on portable devices and media, such as CDs, USB memory sticks, flash drives, PDAs, and portable hard drives. PII should be encrypted on the devices then permanently redacted when no longer needed.
- ✓ If you are unsure about how to comply with requirements, ask your manager, or Security or Privacy Officer.