**West Virginia Executive Branch**
**Privacy Tip**

## Shredding – What's the fuss?

- In December of 2015, California's Attorney General Kamala D. Harris and Alameda County District Attorney Nancy E. O'Malley announced a $26 million settlement with Comcast Cable Communications LLC to resolve allegations that Comcast both unlawfully disposed of hazardous waste, and discarded records containing sensitive customer information, including names, addresses and phone numbers, into the trash without shredding them or making them unreadable, potentially exposing the information to identity thieves.

- One of the largest HIPAA breaches reported in 2016 stemmed from a 2015 incident where paper records were found on the street.
  Radiology Regional Center of Florida notified 483,063 individuals that their information may have been exposed after "a small quantity of records" fell onto the street while being transported by the company responsible for the disposal of Radiology patient records.

- In 2012, it was reported that confetti found at the Macy's Thanksgiving Day Parade was made from shredded police documents. The documents contained confidential information, including detectives' Social Security numbers, bank information and unveiled undercover officers' identities, WPIX-TV, New York, reported. The documents were "strip-shredded" which, if not done properly, may produce strips of documents that can be read.

When documents containing personally identifiable information (PII) including protected health information (PHI) are being disposed of, you must ensure that the documents are rendered unreadable. You should never just throw paperwork away when it could contain such private data. Criminals will sometimes look in trash cans for papers containing PII because they know it can be used to steal someone's identity. It is very important to make sure that both electronic and paper data containing PII is properly disposed of to prevent unauthorized disclosure and use. Shredding can often be your best friend when destroying paper documents.

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

- Know and follow any data retention policies established by your department. These policies will inform you on how long various types of data must be kept.
- Follow the established departmental procedures for securely destroying data. There will be separate procedures for paper and electronic records.
- If you are unsure how to comply with retention and destruction requirements, ask your Privacy Officer.

**Note:** Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.