# E-Waste & Data Sanitization Before Disposal

**Redji Jean Baptiste**  
**ENL1813T**  
**October 5, 2025**

## References

**[1]** Canadian Centre for Cyber Security, "IT media sanitization (ITSP.40.006)," Communications Security Establishment, v2, Jul. 2017. [Online]. Available: <https://www.cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006>. [Accessed Oct. 5, 2025].

This is a primary source from the Canadian government that explains how to properly sanitize and dispose of IT equipment with sensitive data. It covers the legal requirements under PIPEDA and PHIPA, breaks down when you can use software wiping versus when you need to physically destroy hard drives, and shows what documentation you need to keep for chain of custody. This source is directly relevant for understanding the Canadian regulations that apply to decommissioning and figuring out which sanitization method is appropriate based on the sensitivity level of the data.

**[2]** A. R. Regenscheid, L. Feldman, and G. A. Witte, "Guidelines for Media Sanitization," National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-88 Revision 1, Dec. 2014. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf>. [Accessed Oct. 5, 2025].

This is a primary source from NIST that has become the industry standard for media sanitization used by both government agencies and private companies around the world. It breaks sanitization down into three levels - Clear, Purge, and Destroy - depending on how sensitive your data is. This source also explains the technical details of when software wiping is good enough versus when you need to physically destroy or “degauss” the drives.

**[3]** G. Hughes and T. Coughlin, "Tutorial on Disk Drive Data Sanitization," Center for Magnetic Recording Research, University of California San Diego, San Diego, CA. [Online]. Available: <https://cmrr.ucsd.edu/_files/data-sanitization-tutorial.pdf>. [Accessed Oct. 5, 2025].

This is a secondary source from a university research center compares different ways to wipe data from hard drives, including how long each method takes, how secure it is, and whether data can still be recovered afterwards. The tutorial also talks about the legal consequences of improper disposal under laws like the Health Insurance Portability and Accountability Act (HIPAA) and compares old methods like the DoD standard to newer techniques like Secure Erase commands. This is useful for understanding the technical side of data sanitization and making informed decisions about which method to use for the desktop computers based on what type of drives they have and how sensitive the data is.