Data Destruction Information and References

Below is a short technical write up with links to Federal Sources on data destruction requirements for EPHI. The short version is that the required standard is that EPHI must be "purged" via some **physical means** rather than simply overwritten/deleted to comply with HIPAA requirements. If we have a BAA (IIRC we have a standard BAA) with a vendor then in theory they are contractually obliged to follow through because of section 10.

In the HIPAA Disposal FAQ it is indicates that PHI must be "Purged" and references both

- For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

HHS HIPAA Security Series 3: Security Standards – Physical Safeguards with the following criteria for reuse

- Are procedures developed and implemented for removal of EPHI from electronic media before re-use?
- Do the procedures specify situations when all EPHI must be permanently deleted or situations when the electronic media should only be reformatted so that no files are accessible?

NIST SP 800-88, Guidelines for Media Sanitization

- Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort. The level of effort applied when attempting to retrieve data may range widely. For example, a party may attempt simple keyboard attacks without the use of specialized tools, skills, or knowledge of the media characteristics. On the other end of the spectrum, a party may have extensive capabilities and be able to apply state of the art laboratory techniques. *Clear, Purge, and Destroy* are actions that can be taken to sanitize media. The categories of sanitization are defined as follows:
  - *Clear* applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
  - *Purge* applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
  - *Destroy* renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

List of P&Ps and SOPs that might be helpful

- 737 Information Disposal
- 741 System Planning and Acceptance – This also states when a security plan is needed.
- SOP-Information Disposal – very rough outline and not specifically stating vendor
- SOP-User Access Management