Explanation of proper protocol for Government

Regulations in regards to Data Sanitization

Electronic Data Destruction

What are the Regulations?-

Any company which is handling personal information from, or belonging to, a client, or customer, will be held to protect that information from being leaked to an unwanted source. The statute set maintains that a company must use a risk-based process and implement "reasonable" or "appropriate" measures to keep personal information safe and secure. If any information would be leaked, and a client thereby harmed in the process, the company in question would be in violation of the previous obligations and subject to a lawsuit.

What is Reasonable or Appropriate?-

The legal standard has not set in place a specific list of instructions as to which a company must adhere to and insure compliance. The catch it that this open ended "protection plan" leaves a corporation at risk of violating their obligations in many ways, and thus different lawsuits have arose. As a company whole a risk assessment must be performed to discover possible threats to personal information and once they are identified a system of safeguarding each weak point must be documented, set in place and maintained. The NIST (National Institute of Standards and Technology) has taken into account all governing regulations and compiled a distinct set of instructions for all types of medial sanitization, to aid companies in remaining compliant and avoiding potential breaches. By using a product that is compliant with the NIST regulations you can insure that you are maintaining "reasonable" and "appropriate" measures of security. "One method to sanitize media is to use software of hardware products to overwrite storage space on the media with non-sensitive data"[1]

What Information needs to be secured?-

Just as you would want to keep all company data protected from potential theft, any information you deal with from an outside source provides a company with a potential liability of non-compliance. "The statues generally apply to unencrypted sensitive personal information; for example, Information consisting of first name or initial and last name, plus one of the following: Social Security number; driver's license or other state ID numbers; or financial, credit card , or debit card account number."[2]

Appendix: Sources
1-http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf
2-http://www.infoworld.com/d/security-central/data-security-what-law-requires-it-052?page=0,0