Standards Compliance

Your customers depend on you!

support@SCVdata.com
(661) 600-5333

SCVdata helps companies understand how to be compliant with the technical requirements for their industry. There are a number of precautions and backup requirements that companies need to adhere to when they handle sensitive information. Here are some examples of requirements placed upon some of our clients:

• Sarabanes-Oxley Act of 2002

US Congress passed to ensure data and financials are properly being handled. In other circles, this is referred to as the Public Company Accounting Reform and Investor Protection Act of 2002. This is often regarded as the most significant financial reform to US Securities law since 1930's. It ensures the integrity of financial statements. Computer technology is used for most of these controls.

• HIPAA

Health Insurance Portability and Accountability Act for medical records. The privacy portion of this act took effect in 2003 and the security portion took effect in 2005. It involves controlling, securing, managing medical data. The security rule of HIPAA is designed to assure the confidentiality and integrity of Protected Health Information (PHI). The privacy rule of HIPAA is intended to protect the privacy of all Individually Identifiable Health Information (IIHI).

• FACTA

The Fair and Accurate Credit Transactions Act (FACTA) of 2003 came into effect in 2005 (Extension of the Fair Credit Reporting Act (FCRA). Requires that you "take reasonable measures to protect against unauthorized access or use of the information." Also discusses destruction methods of shredding and erasing electronic data. Beyond credit bureaus, banks, and retailers... this may apply to anyone that has done background checks on employees and job applicants.

• USA Patriot Act

Financial Modernization Act of 1999. 3 Sections:
1: Financial Privacy Rule - regulates collection/disclosure of private financial information, 2: Safeguards Rule - financial institutions need security programs, 3: Pretexting Provisions - prohibit accessing private info using false pretenses. Section 6805 (a) is particularly important for IT dictating the need for administrative, technical, and physical safeguards.