

## **Glossary of Common Business Regulatory and Industry Standards**

### **Sarbanes-Oxley Act of 2002**

The Sarbanes-Oxley Act of 2002, sponsored by US Senator Paul Sarbanes and US Representative Michael Oxley, represents the biggest change to federal securities laws in a long time. It came as a result of the large corporate financial scandals involving Enron, WorldCom, Global Crossing and Arthur Andersen. Effective in 2006, *all* publicly-traded companies are required to submit an annual report of the effectiveness of their internal accounting controls to the SEC.

Provisions of the Sarbanes Oxley Act (SOX) detail criminal and civil penalties for noncompliance, certification of internal auditing, and increased financial disclosure. It affects public U.S. companies and non-U.S. companies with a U.S. presence. SOX is all about *corporate governance* and financial disclosure.

### **Gramm Leach Bliley Act (GLBA)**

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC.

[Click here to link to more information on GLBA from the FTC.](#)

### **Health Insurance Portability and Accountability Act (HIPAA)**

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services (HHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

HIPAA compliance can be summarized by the three major rules or standards:

### **HIPAA Privacy Rule**

The HIPAA Privacy Rule mandates the protection and privacy of all health information. This rule specifically defines the authorized uses and disclosures of "individually-identifiable" health information.

### **HIPAA Transactions and Code Set Rule**

The HIPAA Transaction and Code Set Standard addresses the use of predefined transaction standards and code sets for communications and transactions in the health-care industry.

### **HIPAA Security Rule**

The HIPAA Security Rule mandates the security of electronic medical records (EMR). Unlike the Privacy Rule, which provides broader protection for all formats that health information make take, such as print or electronic information, the Security Rule addresses the technical aspects of protecting electronic health information. More specifically, the HIPAA Security standards addresses these aspects of security:

- » **Administrative security** - assignment of security responsibility to an individual.
- » **Physical security** - required to protect electronic systems, equipment and data.
- » **Technical security** - authentication & encryption used to control access to data.

[Click here for more information on HIPAA](#)

## **21 CFR Part 11**

21 CFR Part 11 Sets standards for using electronic signatures and maintaining records electronically in FDA-regulated industries. Title 21, Code of Federal Regulations, Part 11 enables the pharmaceutical industry and other FDA-regulated industries to streamline processes and reduce costs by establishing criteria for the use of electronic records and signatures. For companies that meet Part 11 compliance, electronic records and signatures can replace traditional paper records and signatures.

## **NERC 1200**

Founded in 1968, the North American Electric Reliability Council (NERC) sets industry standards and guidelines for electric utilities. NERC's mission is "to ensure that the bulk electric system in North America is reliable, adequate and secure."

Compliance with NERC standards is becoming mandatory for all electric utilities in North America, with support from all 10 Regional Reliability Councils, the Federal Energy Regulatory Commission (FERC), and North American Energy Standards Board (NAESB).

For more information, visit the NERC website at [www.nerc.com](http://www.nerc.com).

### **Visa Cardholder Information Security Program (CISP)**

The Visa Cardholder Information Security Program (CISP) applies to any entity that stores, processes, or transmits Visa cardholder information. This is part of the Payment Card Industry (PCI) Data Security Standard (DSS).

CISP consists of twelve basic requirements for safeguarding account data, supported by more detailed sub-requirements. These data security requirements apply to all members, merchants, and their service providers. Validation of compliance, however, is prioritized based on the volume of cardholder data and the potential risk introduced into the Visa system by merchants and service providers.

[Click here for more information on CISP.](#)