Government Regulations

What is HIPAA Compliance?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules were signed into federal law in 1996. HIPAA was created to combat fraud and abuse in the health insurance industry. The Act stipulates that all United States health care organizations must “maintain reasonable and appropriate, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information.”

HIPAA protection attaches to all information relating “to the past, present, or future physical or mental health or condition of an individual, or the past, present, or future payment for the provision of healthcare.” Materials that would contain such protected information include patient histories, logs, notes, forms, billing and insurance information, and any other records containing personal information in the possession of healthcare providers.

Regardless of size, all healthcare providers in the United States must have documented policies defining reasonable measures that are being taken to protect personal health information and ensure the organization is protecting against unauthorized access to personal information. This includes all organizations or individuals who retain and/or collect health-related information, such as:

- Hospitals
- Medical Centers
- Insurance Companies
- Billing Centers
- Collection Agencies
- Doctors, Dentists, Chiropractors, Psychiatrists, Psychologists and any other institutions or individuals responsible for personal health-related information

What is FACTA?

Fair and Accurate Credit Transactions Act (FACTA) is federal legislation that was signed into law on December 4, 2003. It was aimed at the prevention and penalization of consumer fraud and identity theft. Administered by the Federal Trade Commission (FTC), the FACTA Disposal Rule has been in effect since June 1, 2005. The Disposal Rule puts in place requirements for proper document disposal and destruction, and recognizes the problems that can and do arise when private information is disposed of in an irresponsible manner. FACTA applies to all persons and businesses in the United States, mandating that "any person who maintains or otherwise possesses consumer information, or any compilation of consumer information, for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."

Under FACTA, consumer information is defined as personal identifying materials which extend beyond just a person’s name, including:

- Social security number
- Driver’s license number
- Phone number or e-mail address
- Physical address

To comply with the FACTA Disposal Rule, businesses and individuals must take "reasonable measures" to ensure such information does not fall into the wrong hands. Reasonable measures include the “burning, pulverizing, or **shredding**” of paper documents, such as the contracting of a third-party engaged in the document destruction business to dispose of confidential information in a manner consistent with the Act.

What is GLBA?

Also known as the Financial Services Modernization Act, the Gramm-Leach-Bliley Act (GLBA) was enacted in 1999 to protect private consumer information held by financial institutions. The GLBA requires banks to develop privacy notices and to provide customers with the option of prohibiting the sharing of their confidential information with non-affiliated third parties. On July 1, 2001, the Act was amended, requiring financial organizations to have a comprehensive, written information security program in place.

What is ITEP?

Identity Theft Enforcement and Protection Act of 2005 mandates that businesses have a legal duty to protect and safeguard sensitive personal information.

Similar to the Gramm-Leach Bliley Act, the ITEP Act requires businesses that collect or maintain sensitive personal information in the regular course of business to implement and maintain reasonable procedures and corrective measures to protect and safeguard sensitive personal information from unlawful use or disclosure. Furthermore, the ITEP Act includes a "Dumpster Diving" provision where companies are required to destroy customer records no longer in use by shredding, erasing or modifying the records to make the information unreadable or undecipherable.