

InfoTrak

Information for Better Decisions



Privacy and Security: What's the Risk to Your Company?

In today's world a tremendous amount of confidential and sensitive information is collected during the normal course of business. This information encompasses financial account information, social security numbers, medical conditions, phone and email addresses and other personal information that is usually captured in client records, payroll records, human resource records, patient records, bank statements, forms and applications—not to mention sensitive company information that may be distributed as a result of discussions, sharing of databases for purposes of subcontracting services or via Web site or tradeshow inquiries.

Recently, there have been a number of new laws and regulations enacted

regarding the protection and handling of customer and patient information. Additionally, there have been high profile cases of corporate information being exposed as a result of various "leaks" where deficient (or non-existent) company policies and procedures existed.

No company can afford the steep fines associated with non-compliance with international, federal and state regulation nor do companies want to jeopardize their market value by allowing information such as price lists, contracts, or client lists to fall into the wrong hands. Security is a tradeoff between managing risks and costs. But all **personal information**, be it information on your employees or customers, is subject to government regulations.

Managing information is not just a matter of setting up controls for the way information is gathered—companies need strict and prudent policies and partners to help manage the way information is stored, distributed, and ultimately disposed of. This is why selecting a fulfillment provider knowledgeable on the evolving regulatory climate and dedicated to the secure protection of your business information is of mission-critical importance.

Regulations that Affect Business

There are several main federal and international regulations that govern the protection of private information. These regulations, listed on page 2, drive the need to have a reliable, secure fulfillment program in place, performed by a company that is knowledgeable about the requisite privacy law requirements and that will assist you in ensuring that you remain legally compliant.

Gramm-Leach-Bliley (GLB) Act: This Act requires that financial institutions take steps to ensure the security and confidentiality of its customers' nonpublic personal information including personally identifiable information such as social security numbers, passwords or access codes for bank accounts, credit cards, ATM cards, financial assets of an individual, consumer credit reports, financial account numbers for an individual, and other similar such financial information that is attributable to a particular individual. The harm caused by "identity theft" has led the federal government to create mandates such as this in order to prevent even the negligent disclosure of sensitive personal information.

Securities Exchange Commission (SEC) ~ Regulation S-P: The purpose of this Regulation is to bring the businesses regulated by the SEC into compliance with the concepts for privacy outlined under the GLB Act. This Act applies to broker-dealers, funds, registered advisers, those who deal with variable annuity or variable life insurance, and any other entities dealing in securities.

Health Insurance Portability and Accountability Act of 1996 ("HIPAA") ~ The Final Privacy Rule: This Rule limits the use and disclosure of individually identifiable health information relating to the physical or mental health of individuals absent consent or authorization from the patient and subject to certain other exclusions.

Safe Harbor Privacy Principles: In October 1998, the European Union's wide-sweeping privacy legislation—called the European Union Data Protection Directive—became effective. The Directive places new requirements on businesses that wish to collect, process or transfer personal data from an EU Member State to a non-EU Member State. Under the Directive, the transfer of personal information from an EU Member State to a non-EU country is forbidden unless the country and the company involved provide an "adequate" level of privacy protection. The EU does not currently view the United States as having an adequate level of protection. In order to avoid potential disruptions in trade between the United States and the EU, the U.S. Department of Commerce, in consultation with the European Commission and the industry, developed the safe harbor framework as one means by which companies can qualify as providing an "adequate level of protection" for such EU personal data.

It is important to keep in mind that "personal data" under the EU Data Protection Act is very broadly defined. It includes the following types of information:

- **Personal Details:** Names, addresses, contact details, age, sex, date of birth, physical descriptions, identifiers such as national health identifying numbers or Social Security numbers. There are certain limited exceptions for information that is essential in order for businesses to conduct business with one another.
- **Family, Lifestyle and Social Circumstances:** Current marriage and partnerships and marital history, details of family and other household members, habits, housing, travel details, leisure activities, membership of charitable or voluntary organizations and similar such information.
- **Education and Training Details:** Academic records, qualifications, skills, training records, professional expertise, student records, and the like.
- **Employment Details:** Employment and career history, recruitment and termination details, attendance record, health and safety records, performance appraisals, training records and security records.
- **Financial Details:** Income, salary, assets and investments, payment status and creditworthiness, loans, benefits, grants, insurance details and pension/retirement information.
- **Goods or Services Provided:** Details of the goods or services supplied, licenses issued, agreements and contracts.

Moreover, sensitive data is subject to further restrictions regarding the transfer of such information. Sensitive data typically includes data relating to an individual's: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sexual preference.

Again, based on the broad definitions of data, which is subject to the terms of the EU Data Protection Act, it is most likely that a majority of companies based in the United States will be subject to some of the EU privacy requirements.

In addition, there are a myriad of individual State legal requirements that require any company wishing to do business in those states to follow those local privacy guidelines and controls. As in the case of the Final Privacy Law of HIPAA, any state privacy laws that are more onerous than the Final Privacy Law of HIPAA will, in fact, preempt the Final Privacy Law, subjecting companies to compliance of the more onerous requirements of the State law. This preemption makes compliance all the more difficult—and critical.

Examples of Industries and Services that NEED Secure Handling Procedures and a Secure Fulfillment Partner

Finance: 401(k) and retirement benefits departments, banks, investment companies, mortgage companies, and securities firms all gather a tremendous amount of personal and confidential information that is legally required to be correctly handled. No financial service provider can risk the exposure generated by sloppy document handling and fulfillment.

Health Care: Pharmaceutical and biotech companies, doctors' offices, hospitals, insurance companies, and medical groups are fast feeling the pressure to become HIPAA compliant. These businesses not only owe it to their patients, both from an ethical and legal perspective, to safeguard confidential and sensitive information, they owe it to themselves not to destroy their name and goodwill because of careless business practices.

High-Tech: It seems that the high-tech industry moves faster and creates more change than any other industry. Product sheets, specification sheets, and documents containing source codes make up the lifeblood of the industry. Losing this information to competitors can literally mean the difference between shareholder return and an unpleasant financial statement.

Other Businesses: Businesses of all types—including accounting firms, employment agencies, payroll processors, colleges/universities and many more—gather, store, and distribute sensitive and private information that is damaging if it falls into the wrong hands. Regulations such as SEC, HIPAA, GLB and the EU provide unwavering guidelines regarding the safeguarding of this information. It behooves any savvy agency to take the necessary steps to conform and remain legally compliant.

How a Fulfillment Partner Can Help

Your fulfillment partner can truly help you and your business comply with regulations and safeguard important company secrets and customer and employee information. Some areas to consider include:

- **Physical Safeguards and Software to Ensure Security:** Partnering with a company that has comprehensive privacy and security programs (including Safe Harbor certification allowing it to receive and protect your EU data) that spans physical, virtual, and personnel, with an added perspective in virus and unauthorized access (hacking), makes sound business sense. Some examples include:
 - ✓ Alarmed facilities with video monitoring
 - ✓ Thoroughly screened personnel including background checks and testing
 - ✓ All employees required to wear ID badges
 - ✓ All contractors and visitors required to sign in and wear ID badges
 - ✓ Strict adherence to procedures and policies
 - ✓ Standardized and reliable information retention and secure information destruction programs

- ✓ Carefully controlled physical access to key computer systems
- ✓ Virtual security with passwords that are required to change on a regular basis, and strict permissions, rights, and levels based on client requirements
- ✓ Anti-virus software at the server and desktop level, regular anti-virus updates, and frequent updates and patches to operating systems software
- ✓ Disciplined enactment of firewall protections and rules
- ✓ Regular internal audits ensuring testing and compliance
- ✓ Annual re-certification regarding Safe Harbor Certification to ensure adequate protection of EU personal data.
- ✓ Global expertise regarding privacy requirements.

• **Secure Transfer, Usage and Destruction of Data:**

It is crucial that the “Chain of Custody” be controlled from the time information leaves your secure location, through the data manipulation, printing and shipping at the fulfillment vendor, to the eventual secure destruction of the source information.

Data that is sent to your fulfillment partner during the normal course of business may include transfers via phone, fax, e-mail, a secure-FTP (file transfer protocol) file or an XML interface using SOAP techniques. A secure FTP automatic transfer using SOAP can dramatically improve the confidential linkage and integration with client systems, and ensure that only “authorized” personnel are viewing sensitive documents. Your fulfillment partner should have applications that offer proven and secure solutions that will interface to sales force automation and customer relationship management (CRM) systems.

File systems that store your confidential data should have access controls over them as well as have regular destruction purges applied to them based on pre-defined retention standards. This will ensure that only authorized personnel can use the data during its intended life and that confidential data cannot be inappropriately accessed.

• **Commitment to Mutual Success:**

Your fulfillment partner should have a documented plan based on a commitment to mutual success. For instance, employees that are recognized, both verbally and financially, based on their efficiency, accuracy, and effectiveness, tend to view themselves as partners. Strive to find a fulfillment company that treats its employees as partners, which will help to ensure your overall success.

Your business and customer information is too valuable to not properly protect; and your risk of lost reputation and trust as well as steep fines too great to jeopardize. For more information on how to reduce your risk through proper compliance with laws and regulations through a secure fulfillment program, or for a detailed document on the regulations discussed in this issue, please contact David Lowndes, Director of Product Development, at 512-719-9806.

What types of information need special handling and protection...

- Contracts
- Customer information
- Customer lists
- Phone and email information
- Medical histories
- Financial account information
- ID badges
- Inventory lists
- Legal documents
- Marketing plans
- Meeting minutes
- Microfiche
- Payroll records
- Personnel files
- Price lists
- Product proposals
- Research & development records
- Strategic Plans
- Tax records
- Time sheets



Corporate Headquarters:
 Comac, Inc.
 565 Sinclair Frontage Road
 Milpitas, CA 95035
 1-866-COMAC4U
 www.comac.com