



# PRIVACY: FROM CONSUMER CONCERNS TO COMPLIANCE STRATEGIES

## — And The Role of RIM

According to the Privacy Rights Clearinghouse, in 2005, approximately 3.9 million customer banking records were jeopardized when a back-up computer tape was lost, leaving the responsible financial institution liable for recovering the lost data. That same year, another large banking institution suffered a similar fate when a misplaced back up tape compromised more than 1.2 million customer records.



### INSIDE THIS ISSUE:

Privacy: From Consumer Concerns to Compliance Strategies.....1-6

Strategies and Practices for Handling Confidential Information .....2-5

Understanding the Regulatory Guidelines Impacting Privacy.....3

Solutions for Securing Physical Records and Maintaining Privacy.....4

SYSTEC Solutions.....5

Ask the Expert .....6

Significant media coverage generated considerable concern among the public, which continues to increase as more and more personal information is regularly shared with businesses. For organizations gathering confidential information, maintaining privacy has become an organizational and regulatory issue. Understanding the concerns of your customers, the guidelines governing your liability, and the steps needed to protect confidential information is key to ensuring privacy and protecting your organization from the consequences of non-compliance.

### Consumer concerns

A recent Harris Poll revealed that 94 percent of Americans are concerned about the possible misuse of their personal information by businesses. This staggering percentage only validates the challenges facing organizations to gather, retain, utilize and disclose information while still maintaining consumer trust. Individuals want those organizations that request their personal information to provide the necessary safeguards to ensure confidentiality and effectively communicate those details to establish a level of trust. Most importantly, consumers expect businesses to be held accountable when their privacy is not protected.

# STRATEGIES AND PRACTICES FOR HANDLING CONFIDENTIAL INFORMATION

*The protection of private information is a challenge facing businesses of all sizes. While organizations depend on gathering confidential data, protecting and controlling the way that information is stored, accessed and secured is becoming a more complicated undertaking. Putting the necessary tools, processes and procedures in place to protect information, meet regulatory compliance guidelines and reduce liability is an important piece of the record security puzzle.*



## Storage solutions

Physical, secure storage of paper records and archived formats such as microfilm, CDs and tapes, can be achieved using various storage solutions, including locking cabinets and shelving units (see page 4 for more information). By centralizing and securing confidential information in locking storage units, its safekeeping is ensured and controlling the information is easier.

## Record management technologies

Another effective method of maintaining the privacy of confidential paper records is the use of tracking technologies. Barcode tracking and RFID technologies allow for accurate and efficient management of records as they move throughout an organization, as well as ensure information is appropriately accessed. These technologies track what records have been accessed and when, as well as who accessed them and for what purpose.

## Electronic document management

When dealing with confidential electronic records, computer system security is critical to data protection. Secure electronic data by installing read-only and password protected programs to prevent unauthorized access and data duplication. Store active data on secure servers and archive digital media in locking cabinets (see page 4 for more information).

## Internal practices

While having appropriate storage systems, tracking technologies, and EDM systems in place is critical to the management of confidential information,

implementing solid internal processes to maintain them will add the final level of control.

The first step in implementing best practices is dedicating an individual or team of individuals to develop and/or manage a compliant and secure records and information management system. Many companies rely on RIM professionals, IT personnel or administrative professionals to handle this responsibility. In recent years, Chief Privacy Officers have been instituted to manage and protect confidential information, as well as develop policies and procedures that more effectively address privacy-related issues (see sidebar article).

Developing the internal policies and procedures to manage record confidentiality requires an in-depth understanding of privacy-related regulatory guidelines that impact your industry (see page 3 for more information.) In addition, all internal privacy directives already in place should be evaluated to ensure compliance with any recently amended regulatory guidelines.

Next, identify the records within your organization that require security, such as human resource files, client documents, accounting files or any other business critical records that could impact regulatory compliance or present a liability when inadvertently disclosed. Consider bringing in an outside resource to help with the identification process and ensure that all appropriate documents are

# UNDERSTANDING REGULATORY GUIDELINES IMPACTING PRIVACY.

*The first step in securing your company's vital records involves researching the various types of government regulations and identifying those that pertain to your industry. Understanding the nuances of those guidelines can help you better implement the appropriate policies and procedures to increase your compliance and decrease your liability.*



- **Gramm-Leach-Bliley Act** – Governs the collection and disclosure of customers' personal information by financial institutions, such as banking and lending institutions, securities firms and insurance companies. It also applies to companies, whether or not they are financial institutions, which receive such information, including companies providing other types of financial products and services to consumers, such as loan officers, tax accountants, financial consultants, real estate brokers and debt collectors. *For more information on the Gramm-Leach-Bliley Act, go to <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>.*
- **The Privacy Act of 1974** – Provides for the security of all forms of an individual's personal information and proper disclosure of that information by federal government agencies. Agencies regulated by the act must securely store personally identifiable information, advise individuals of policies regarding the sharing of information and give them the option of refusal for information sharing. *For more information on The Privacy Act of 1974, go to [www.usdoj.gov/foia/privstat.htm](http://www.usdoj.gov/foia/privstat.htm).*
- **The HIPAA Act** – Protects all forms of personal health information about a patient that is maintained or received from a healthcare provider, hospital, health plan or insurer, health claims processors, pharmaceutical companies, and other treatment providers. Specifically, HIPAA requires the protection of individually identifiable health information and is designed to ensure confidentiality, integrity and availability of electronic patient information. *For more information on HIPAA, go to [www.ahima.org](http://www.ahima.org).*

# SOLUTIONS FOR SECURING PHYSICAL RECORDS AND MAINTAINING PRIVACY.

*Ensuring the confidentiality of your vital paper records and electronic data begins with the use of appropriate storage methods. Locking cabinets and secure shelving units add a higher level of control to your records management needs. With an array of secure storage systems available, SYSTEC professionals can recommend and provide the right solution for you.*



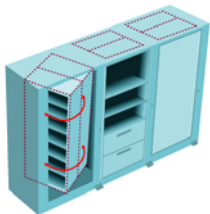
## High-Density Mobile Systems

Mobile systems can be rolled together and locked down during off hours or when not in use to create a space-efficient and secure storage solution.



## Lockable File Cabinets

Cabinets can be secured by locking individual drawers or an entire unit can be secured using an interlocking mechanism to safeguard multiple drawers within the cabinet.



## Rotary File Units

These space-efficient lockable storage solutions can be outfitted in an array of configurations to provide compact, back-to-back, secure storage of any confidential material.



## Tambour Doors and Flipper Doors

Locking tambour doors may be added to any freestanding shelving range or mobile storage system and lockable flipper doors can be hung on file cabinets or mobile shelving units to protect vital records and materials.



## Secure Media Cabinets

Freestanding cabinets, lateral storage and high-density media storage, offer a space efficient, secure design to protect an assortment of media including audio and videotapes, CDs, DVDs and microfilm.

### Filing system security

Evaluate your existing paper-based filing system to determine whether or not your approach lends itself to a high level of security. For example, replace confidential files categorized by identifiable information, such as first and last name or social security number, with a color-coded filing system that is numerically sequenced. Transfer confidential data from basic filing cabinets or open shelving to locking storage systems located in a secure, centralized file room.

### Written policies and procedures

Once all of these steps have been taken, create a written plan that outlines procedures that include how confidential information should be gathered, processed and secured. Define who should have access to the information and how it should be managed once it is accessed. Include retention guidelines for private records, as well as processes for record destruction. Outline a plan for informing consumers of the steps being taken to ensure their privacy and make sure the plan is accurately followed.

In today's information-sensitive environment, protecting confidential information is becoming a critical business strategy, as well as an ethical and regulatory issue. By implementing and continuously evaluating storage methods and privacy-related policies and procedures, organizations can ensure their compliance while reducing their liability, and consumers can rest assured that their personal information is in trustworthy hands. ■



#### What is a CPO?

A Chief Privacy Officer (CPO) is an individual that focuses his or her attention on the correct use of confidential information within an organization. This position is often found in industry sectors such as finance, healthcare, insurance, telecommunications and consulting. The background of a CPO may include a degree in information technology or business ethics; experience working with government agencies; and an understanding of business process management. Responsibilities of this position may include:

- *Monitoring RIM systems and business processes to ensure information security and regulatory compliance*
- *Ensuring the privacy of the organization's customers, employees, vendors and suppliers*
- *Training staff on privacy issues and internal processes*
- *Developing and implementing privacy-sensitive policies and procedures*
- *Working with government agencies on privacy-related issues*

## SYSTEC SOLUTIONS *ENSURING INFORMATION PRIVACY*

Whether you are protecting personal health information, financial documents, employee records or other critical data, maintaining regulatory compliance and ensuring privacy is essential. SYSTEC professionals can help you evaluate your current processes and procedures to determine your level of compliance and provide you with everything from secured storage and color-coded filing systems to barcode labeling and document tracking systems to protect and accurately manage your confidential records.

**For more about how SYSTEC can help you with your filing system needs, call 1-877-7SYSTEC or e-mail us at [info@systecgroup.com](mailto:info@systecgroup.com). ■**

### Compliance regulations

The government is keenly aware of the growing public concern over privacy protection, and the number of confidentiality-related regulations continues to rise. Between HIPAA, which protects a person's medical information, and Gramm-Leach-Bliley, which protects a person's financial information, government regulations provide a safeguard for consumers and businesses alike. Consumers are guaranteed that the information they provide is secure, and organizations have the guidelines in place to reduce liability and position themselves as reliable in the use and disclosure of secure information.

### What can RIM Professionals do?

RIM professionals have a fundamental responsibility to manage and protect confidential consumer information. Each organization should take into consideration its own internal business practices, as well as regulatory compliance, when developing and implementing privacy policies and procedures. It is the role of the RIM professional to also ensure that the practices put in place are accurately followed and safeguards are in place that will help maintain regulatory compliance and reduce any liability. ■

### WHAT CONSTITUTES A CONFIDENTIAL RECORD?

Any record to which public access is or may be restricted or denied by state or federal law.

For example:

- Employee/HR files
- Accounting records
- Medical records
- Loan applications/mortgage documents
- Bank statements
- Customer account records
- Employment applications
- Credit applications/reports
- Any records containing personally identifiable information like a social security number

**CONFIDENTIAL**

### Ask the EXPERT



*Ask the Expert is your opportunity to receive information management advice from industry experts. From new technology to process improvements, you will learn ways to capitalize on information assets. If you have a question, visit [www.systecgroup.com](http://www.systecgroup.com) and follow the Ask the Expert link. Your question will be answered in about a week.*

**Q:** We are a small, private health-care clinic in need of implementing processes to meet HIPAA compliance guidelines. Where do we start?

**A:** Understanding how HIPAA impacts your organization, as well as what steps you need to take to comply, is key to eliminating liability and noncompliance. Begin by familiarizing yourself with HIPAA guidelines, such as the type of personal health information that needs to be protected. Visit <http://aspe.os.dhhs.gov> or [www.hipaa.com](http://www.hipaa.com) for detailed information. Evaluate internal operations to understand the impact HIPAA will have on your current practices. Review and document your security policies and procedures. Develop a privacy plan and implementation procedures that include securing patient records that contain individually identifiable health information. Designate individuals and vendor partners to oversee plan implementation and provide the products and services necessary to comply. Finally, inform patients of their rights and the steps you intend to take to safeguard their personal health information. ■



**SYSTEC**™  
systems ♦ technology  
[info@systecgroup.com](mailto:info@systecgroup.com)  
[www.systecgroup.com](http://www.systecgroup.com)  
1-877-7SYSTEC

For a **FREE** online subscription, go to: <http://www.systecgroup.com/newsletterform.asp>

Please send your editorial contributions or requests for printed copies of the newsletter to: [info@systecgroup.com](mailto:info@systecgroup.com)

To unsubscribe to this newsletter, e-mail a blank message to: [unsubscribe@systecgroup.com](mailto:unsubscribe@systecgroup.com)