Record Master Risk Management System

Protecting the information you need to do business

18 Identifiers that must be protected

1. Name
2. Address
3. Any date related to the individual
4. Telephone numbers
5. Facsimile numbers
6. Email address
7. SS#
8. Medical record numbers
9. Health plan beneficiary number
10. Account numbers
11. Certificate / license numbers
12. Vehicle identifiers and serial numbers
13. Device identifiers and serial numbers
14. URLs
15. IP address numbers
16. Biometric identifiers including fingerprints and voice prints
17. Any full face photos
18. Any other unique identifying number

Updated 03/10/10

Responsible Record Management

Considering information security, government regulations, customer confidence, and the cost of identity theft, record management is a high priority in today's business world. This can be an enormous challenge for the person assigned to oversee the record management policy, considering limited budgets and time. Being proactive to reduce risk is vital, no matter what your industry.

Government Regulations

A common misconception is that the **HIPAA Privacy Rule** pertains only to the medical industry. Any employer who offers their employees a medical plan is required to meet HIPAA compliance. As an employer, life insurer, school or university, or health care clearinghouse, you must protect any individually identifiable health information including 18 common identifiers (e.g., name, address, birth date, Social Security Number and others).

Much like HIPAA, The **Sarbanes-Oxley Act of 2002**, also known as ***SOX***, requires extensive safeguards for sensitive information. Any publicly held company failing to comply would face fines and possible criminal charges. SOX requires firms in the financial industry to secure physical and electronic records. Further, they are required maintain a detailed history of not only who has access to the records, but when they accessed them. The individual responsible for SOX compliance must be able to produce an audit report of who has accessed the records upon demand.

C&C SECURITY SYSTEMS, LLC 3960 Industrial Park RD Camp Hill PA 17011 www.cc-security.com

Record Master Risk Management System

Protecting the information you need to do business

Reasons to implement a record management policy

Reduce the chances that your firm will be responsible for identity theft

Every year 10 million identities will be stolen

500,000 medical identities were stolen in 2008

Reduce your chances of costly litigation

In 2003 3 women at a major university were awarded $2.4 million when their medical information was shared with a 3rd party.

Increase customer confidence

Produce audit reports with a few simple keystrokes to show who has accessed clients critical data.

Updated 03/10/10

Why implement a Record Management Ploicy?

Litigation

A properly implemented record management policy will help reduce your potential for costly litigation. Employees are less likely to abuse privileges when they are held accountable for their actions.

In 2003, a lawsuit was filed against a major university when the records of three women were compromised and information was shared with a third party. The women were awarded a $2.4 million settlement.

Identity Theft

Identity theft is still one of the fastest growing crimes in the world. Approximately 10 million Americans each year discover that their personal information has been used to open fraudulent bank accounts, credit cards, utility accounts, or used to commit crimes.

Medical identity theft is growing even faster. Over 500,000 medical identities were stolen in 2008. When a medical record is stolen and misused, it could put the individuals life at risk.

With the exception of hackers stealing hundreds of thousands or millions of records at one time, the majority of identity theft occurs physically. In the case of medical identities, 75% are stolen by individuals with access and sold.

Customer Confidence

Protecting yourself against non-compliance fines, reducing your risk of litigation, and protecting your employees and clients from identity theft are just a few of the benefits of a record management policy.

Perhaps just as important is the confidence your customers have in your company. Not taking proactive steps to prevent identity theft could cause irreparable damage to your firms reputation.

What would your clients say if they learned that it was your firm that allowed their identity to be stolen?

C&C SECURITY SYSTEMS, LLC 3960 Industrial Park RD Camp Hill PA 17011 www.cc-security.com

Record Master Risk Management System

Protecting the information you need to do business

The Pillars of Responsible Records Management.

Accessibility

Accountability

Confidentiality

What is the most important part of any record management policy?

Implementation!

Updated
03/10/10

Compliance

Finding a commonsense policy that will allow you to meet or exceed the government regulations pertaining to proper record management can be daunting. While there are numerous elements to a record management policy, the most important step is implementation. Many firms will spend uncounted hours and money writing and preparing for a record management policy, and will stop short of implementation for numerous reasons.

Here are a few key elements of any good record management policy. You will need to establish:

1. **Administrative Safeguards** - administrative actions, policies and procedures to manage the selection, development and implementation of a record management policy.
2. **Physical Safeguards** - physical measures, policies and procedures to protect physical and electronic records from natural and environmental hazards and unauthorized intrusion.
3. **Technical Safeguards** - the technology, policy and procedures for its use to protect physical and electronic records and control access to it.
4. **Organizational Requirements** - determining the organizations storage requirements for physical and electronic data, ensuring there is adequate capacity for both and finally determining how the data will be secured and later destroyed.
5. **Policies and Procedures** - Writing, ***implementing***, and enforcing the organizations record management policies.
6. **Implementation -** So important it needed to be mentioned again. Many organizations will work hard through steps one through five, but will balk at implementation. There are a number of reasons, but the bottom line is, steps one through five are meaningless if the record management policy isn't put into place.

C&C SECURITY SYSTEMS, LLC 3960 Industrial Park RD Camp Hill PA 17011 www.cc-security.com

Record Master Risk Management System

Protecting the information you need to do business

There are many reasons record management policies fail.

Here are a few.

1. They are too complex. If the staff has to jump through too many hoops to get a record, they will find a way to circumvent the policy.
2. The equipment is too hard to operate. Meaning locking and unlocking filing cabinets every time you need a record is difficult.
3. Failure to implement the policy.
4. Failure to enforce the policy. If the staff learns they can violate the policy with impunity, the will.

Updated
03/10/10

The pillars of responsible records management

Begin by identifying the physical and electronic records that need to be secured and how long you have to keep them. Once you have established the records that need to be secured, you need to take steps to secure them that will meet the applicable government regulations.

Accessibility: A key element to securing the data is to be able to grant easy access to the records by authorized personnel. If gaining access to the records is too complex, individuals will find a way to circumvent the policy.

Accountability: A properly designed access control policy will provide clear accountability of who has accessed the records. It should be a simple process to pull audit histories of who has accessed the records and equally simple to restrict access to the records.

Confidentiality: A properly implemented record management policy will help to protect the personal information your staff and clients have entrusted to your care.

The question is, how do you establish a record management policy that helps to solve your federal compliance issues, reduces the chance of data being misused (identity theft) and is still simple enough that your staff will use it?

C&C SECURITY SYSTEMS, LLC 3960 Industrial Park RD Camp Hill PA 17011 www.cc-security.com

Record Master Risk Management System

Protecting the information you need to do business

Access controlled filing cabinets.

- Compatible with most existing access control systems.
- Grants access using …
  - iButtons
  - HID
  - Proximity
  - Keypads
  - Biometric
  - Smart cards
- Release all drawers with one reader or have an individual reader for each drawer.
- Control multiple cabinets and drawers with a keypad. Add a keypad with a proximity reader for added security.
- Integrated CCTV. Covert cameras can be installed in the cabinet or external cameras can be installed in the room and "attached" to the cabinet by reader.

Updated 03/10/10

Achieving compliance in any industry is now easier with the *Record Master Risk Management System.*

- Secure private information for as long as necessary
- Keep records locked up at all times, granting access to only authorized personnel.
- Provide audit reports upon request.

The *Record Master Risk Management System* allows you to responsibly manage records while taking proactive steps toward regulation compliance and avoiding the mishandling of records that may result in litigation. With a few simple keystrokes within the web-based software, you will be able to:

- Grant access based upon time, day, individual, department, cabinet, and or drawer using access levels that you define.
- Pull audit reports with a few simple key strokes to produce a physical report showing who has accessed the records.
- Enable or disable the users access from any workstation on your network. Keys can be copied, key fobs or cards cannot. Never worry again about lost or copied keys being used to access files. Establish time-zones to lock out access to the cabinets after business hours.
- Integrate CCTV as an added layer of security. Security cameras can be installed in, on or near the Record Master RMS filing cabinets to record who has accessed the records. "Tied" to the readers on the cabinets the system can record the image of everyone accessing the records.
- Operating on the Access Control platform that you already have, the system is also sold with its own access control system. The user friendly system is network based and can be managed from any work station on your network.

For more information, contact C&C Security Systems Today!
888-442-2301 ext 701

C&C SECURITY SYSTEMS, LLC 3960 Industrial Park RD Camp Hill PA 17011 www.cc-security.com