IS YOUR BUSINESS COMPLIANT?

SAFEGUARD DESTRUCTION
SECURE DOCUMENT SHREDDING

ONE BRUSSELS STREET
WORCESTER, MA 01610
P: (508) 795-1015
F: (508) 795-7276

SAFEGUARD DESTRUCTION
SECURE DOCUMENT SHREDDING

ARE YOU COMPLIANT?

Read this explanation of the new data protection laws to ensure your compliance and to avoid serious and damaging penalties that could affect your business.

MASSACHUSETTS GENERAL LAW CHAPTER 93H

This law requires all businesses in Massachusetts to take serious measures to prevent identity theft. Any business holding the name of a Massachusetts resident and their Social Security Number, Driver's License Number, or financial account number (including credit or debit card numbers) is subject to this new Massachusetts data protection law. 93I requires the shredding or destruction of any paper files containing sensitive information and the erasure or destruction of any electronic files or data storage devices containing personal information of employees or customers.

YOU MUST SAFEGUARD

- Social Security Numbers
- Driver's License or State Issued ID Numbers
- Financial Account Numbers
- Credit or Debit Card Numbers

MASSACHUSETTS GENERAL LAW CHAPTER 93I

93I requires the shredding or destruction of any paper files containing sensitive information and the erasure or destruction of any electronic files or data storage devices containing personal information of employees or customers.

93I also requires a written policy regarding the disposal of sensitive information.

WHAT ARE THE PENALTIES?

- A violation of 93H levies fines of up to **$5000** per record compromised.
- A violation of 93I levies fines of up to **$100** per record compromised with a maximum of **$50,000**.
- This does not take into consideration the loss of your company's hard-earned reputation and the potential loss of credit.

Find more information on these laws and other laws that may affect your business on our website at: http://www.safeguarddestruction.com/Resources

SAFEGUARD DESTRUCTION
SECURE DOCUMENT SHREDDING

HIPAA- Are you Compliant?

What is HIPAA?

HIPAA, passed in 1996, stands for the Health Insurance Portability and Accountability Act. This act has evolved over the years and has expanded to impose heavy fines and sanctions on any healthcare provider that does not take the necessary steps and actions required to protect a patient's healthcare information.

HIPAA compliance has become increasingly more difficult to achieve with the recently passed amendments which...

1. Increased mandatory fines 6,000% (from $25,000 to $1,500,000)
2. Made the States' Attorney General now also responsible for enforcing compliance
3. Require practitioners to inform authorities in the event of a Health Data Breach

Who does it affect?

Any healthcare provider or entity that holds Protected Health Information (PHI). For detailed information on PHI, please visit www.properPHIdisposal.net.

What are the penalties of Non- Compliance?

Fines of up to $1,500,000 have now become mandatory in the event of certain violations, specifically including the improper disposal of patient information.

What are you required to do?

Any entity holding PHI must, according to the US Department of Health and Human Services, among many other things,

> "Maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records [with a Records Management company], and limiting access to [medical records] with keys or pass codes".

For more information on HIPAA:

Understanding HIPAA

HIPAA Compliance

93H & 93I- Are you Compliant?

What are the MA General Laws 93H & 93I?

93H requires all businesses and entities in Massachusetts to take serious measures to prevent identity theft. Any business holding the name of a Massachusetts resident and their Social Security Number, Driver's License Number, or financial account number (including credit or debit card numbers) is subject to this new Massachusetts data protection law.

93I requires a written policy regarding the disposal of sensitive information. You will be able to see an example of a written policy (Written Information Security Policy) by viewing Safeguard Destruction's WISP at the end of this packet.

Who do they affect?

Massachusetts General Laws 93H & 93I affect any entity that holds information of a Massachusetts Resident that could lead to the identity theft of that resident. Types of information that could lead to identity theft include financial payment information held by your office or records containing social security numbers.

What are the penalties of Non- Compliance?

- A violation of 93H levies fines of up to $5000 per record compromised.
- A violation of 93I levies fines of up to $100 per record compromised with a maximum of $50,000.
- This does not take into consideration the loss of your company's hard-earned reputation and the potential loss of credit.

What are you Required to do?

- Proper disposal (shredding, pulverizing) of sensitive information
- Have controls on employees' access of sensitive information, including physical security safeguards, computer user access levels and user authentication protocols.
- Detail security measures on computer information systems, including data encryption, anti-virus and anti-spyware software, and firewalls.
- Periodic review of audit trails and monitoring of systems for unauthorized access.

Your Partner in MA GL 93H & 93I Compliance- Safeguard Destruction

Safeguard Destruction can partner with your office to help ensure your compliance with Massachusetts General Laws 93H & 93I by providing secure, documented, and certified shredding of sensitive Massachusetts resident information as well as aiding in the formulation of your own Written Information Security Policy

What is the 93H and 93I accompanying regulation 201 CMR 17.00?

201 CMR 17.00 requires that your organization take three concrete steps to prevent identity theft:

- Appoint an Information Security Manager (ISM).
- Write and approve a written Information Security Policy (ISP).
- Your ISM must help your staff carry out the ISP, and audit compliance regularly.

Please see the information below for a 201 CMR 17.00 compliance checklist as well as an example of an ISP

For more information on MA GL 93H & 93I:

Understanding 93H & 93I

93H & 93I Compliance

For more information on 201 CMR 17.00:

Understanding 201 CMR 17.00

Safeguard Destruction Information Security Policy

Introduction

We are a Records Management and Destruction company doing business in the Massachusetts areas comprised of greater Boston, Worcester and Rt. 495 belt. We have an office and warehouse comprised of 70,000 sq. ft.

We'll first explain what sensitive information is; provide an overview of our daily business, and how we protect it from people committing identity theft and other crimes.

Information on who is responsible for what aspects of information security is in Roles and Responsibilities at the end of this document.

What is Sensitive Information?

Sensitive information is information that is not lawfully available to the public and could be used to damage our customers, our employees, or our business. This includes Personal information most commonly used to commit identity theft and similar crimes, such as a person's name and any of the following:

- Personal identification, including a number or other identifying information from social security, state id card, driver's license, passport, employee id.
- Financial account identification, including bank account number or credit card number.
- Other identifying information to access financial accounts or non-public records, including usernames, passwords, PINs, etc.
- Employee records, including payroll, pension, and insurance.
- Business-private information for legitimate business purposes, including business plans; vendor and customer lists; contracts; and account information of vendors, clients, and customers.
- Financial transactions with our customers, employees, and vendors, including cash, check, and credit card transactions.

Why We Are Responsible for Sensitive Information

The purpose of our business is to provide secure Records Management and Records Destruction. To that end, customers entrust us with personal information acquired from their customers collected while performing their regular business practices. We also store personal information of individuals that may be contained in storage containers given to us by an individual. We store this information responsibly, utilizing high levels of safety and security including camera surveillance, a pass coded main entrance door and limited, controlled accessibility to stored records and fire prevention.

We provide our own NAID certified destruction at our Worcester warehouse location. Records are shredded and then picked up by Northstar Recycling Company of East Longmeadow, MA who is a reputable ISP compliant vendor, providing secure transport of the shredded paper. The shredded paper is further reduced to paper pulp and used in recycling.

In addition, the operation of our business requires customers, employees, vendors, and business partners to entrust sensitive information to us for good business reasons. We store and use that information responsibly, protecting it from unauthorized or illegal use.

Here are some ways we use it:

As required by law, we keep employment records, including payroll records, and tax forms (W-4 and I-9). We also keep information about the health insurance plan we provide for some of our employees.

When a customer pays by check, we ask to see a driver's license or passport, and record the number on the check. We scan the check, endorse it, and deposit at our bank.

When a customer pays by credit card, we examine the customer's ID (for example, driver's license or passport), but we don't record the number. We normally don't record the credit card number (we swipe the card through the reader), but if the reader is unavailable, we record the credit card information and deliver it to our credit card processing service.

Storage and Display of Sensitive Information

- Sensitive information can be stored and displayed on many kinds of media.
- Many of these media are casually removable and portable, including paper, CD, DVD, and flash drives.
- Other media are not as casually removable, including computer internal hard drives.

All media are subject to theft by someone who:

- Breaks or bypasses the visual security of the store or home office, including seeing computer screens, checks, and credit slips of other people
- Breaks or bypasses the physical security of the store or home office; or
- Breaks or bypasses the electronic security of our computers and networks.
- It is our responsibility to make it reasonably difficult for someone to gain access to sensitive information in our possession.

Sharing Sensitive Information with Government Agencies

We routinely share sensitive information with government agencies, which we assume follow information security policies that are legally compliant and over which we have no control.

Sharing Financial Information with Financial Institutions

We routinely share sensitive financial transaction information with our financial institutions, including customer checking account numbers and credit card numbers.

Sharing Sensitive Information with ISP-Compliant Vendors

We routinely share sensitive information in the form of employment records and insurance information, and other information required to be a responsible employer.

We share this with our bookkeeping service, our payroll service, our CPA firm, our legal counsel, and our business advisor. Our computer service company may sometimes see this information in the course of repair work and consulting.

We require each of these organizations to confirm in writing that they follow a written Information Security Plan that fully complies with all governmental laws and regulations for this location, including Massachusetts information security regulations (201 CMR 17), signed by the CEO or other authorized person.

Ensuring That Our Staff Follows Our Information Security Policy

Our Information Security Manager (ISM) trains every new member of our staff in his or her role in carrying out the Information Security Policy (ISP). This training is refreshed at least annually. New staff members agree in writing to follow our ISP and understand that their continued employment in our organization depends on their following the ISP. Employees who fail to follow the ISP are given written warnings, followed, if necessary, by being asked to leave the organization.

A note about the paragraphs that follow - we talk about keeping paper records under lock and key, and computer records restricted to certain users. We use good common-sense practices about this. When we walk away from a Windows computer, we lock the computer by using WindowsKey-L. On a Windows computer that doesn't have a WindowsKey, we lock the computer with Start > Log Off > Switch User

Protection of Sensitive Information

We use good common-sense practices to protect sensitive information:

Regarding records storage, our hiring practices demand criminal background checks on all new employees. Warehouse employees work under stringent guidelines regarding the handling of stored records, prohibiting the unauthorized handling of any stored records except under explicit direction of the Assistant Operations Manager and under the supervision of the Warehouse Manager.

When a customer requests to view stored records, the request must be received 24 hours in advance. An appointment is set, and the files are removed from the warehouse to a secure viewing room. The files do not leave the room unless a written request is made, and a signed receipt is issued for removal from the premises.

Customers are not allowed to drop off boxes or files for storage or destruction.

There is a strict no admittance policy to either the offices or warehouse for anyone other than employees or approved appointments.

- Where reasonable, we store sensitive information in strongly encrypted form so that even if someone steals or accesses the media, they don't have easy access to sensitive information.
- No personal or external laptops or computers are allowed in the facility at any time.
- In both the office and warehouse, we keep all unencrypted and easily removable physical media that contains sensitive information (check, credit slip, CD, DVD, tape, flash drive, paper, microform, etc.) in a locked space where it is reasonably safe from burglary and intrusion. We routinely carry unencrypted media containing sensitive information between the warehouse and office.
- When we use sensitive information, we hold the media and its contents closely, we don't share it inappropriately, and we return it to an appropriate locked space when we're done. For example, we don't leave lying on counters, tables, or desks any unencrypted sensitive information, including checks, credit slips, and file folders containing W-4s and I-9s. We also don't leave sensitive information displayed on an unattended computer screen.

Destruction of Obsolete Sensitive Information

We regularly destroy obsolete records.

We destroy most paper records generated in the office using an office-grade shredder.

We destroy most records on re-writeable media (disk drives, flash drives, etc.) by US-Department-of Defense-compliant overwriting of the information.

We destroy other records in media-appropriate ways, such as physical breakage or delivery to an ISP-compliant information destruction service.

Delivery of Encrypted Sensitive Information

Strongly encrypted sensitive information may be delivered without the associated encryption keys in any medium by any route, including by mail or email.

Strongly encrypted sensitive information and the associated encryption keys may both be mailed only on different days.

Otherwise, encryption keys may only be delivered by fax or phone.

Usernames and Passwords

Usernames and passwords may both be delivered by mail only if they are mailed on different days.

Otherwise, usernames may only be delivered separately by a route of hand, fax, phone, mail, or email; and passwords may only be delivered separately by a *different* route of hand, fax, phone, or mail. Passwords may never be delivered by email.

Financial Transactions

When we receive checks from customers, we keep them in a locked space. The Operations Manager or Assistant Operations Manager is responsible for the security of checks before deposit. (see Roles And Responsibilities).

The Operations Manager, Assistant Operations Manager or Office Manager deliver checks, credit slips, cash, and other financial instruments by hand to an appropriate financial institution, such as our bank or credit card processing service.

Unencrypted employment records are kept in a locked space and accessed only by the staff responsible for employment issues, which in our case are the Operations Manager, Assistant Operations Manager, and the Office Manager.

When a records customer needs to take unencrypted records with sensitive information anywhere not listed above, they must first explain in writing the business reasons that this is necessary, and the Operations Manager must give written permission for the removal of any documents from the premises.

Delivery of Unencrypted Sensitive Information

We deliver unencrypted sensitive information to customers and to ISP-compliant vendors only by hand, fax, mail, phone, encrypted email or ISP-compliant delivery service.

Employment records are kept in a locked space or in a Secure Computer Network. See "Secure Computer Network" below for our practices for keeping our computer network secure.

Emailing Sensitive Information

We email sensitive information between us and our records storage customers, payroll and pension companies, accountant, and bookkeeper only in strongly encrypted form with a password arranged by in-person, fax, or telephone contact.

Strong Passwords

Password must be at least 8 characters, including one punctuation mark and one change of case. The password must be hard to crack by a dictionary attack, so if it has a word or a proper name, it must have at least TWO unrelated words or proper names.

The ISM keeps all passwords in a master password file encrypted with a master password that stored by the Operations Manager. The password list includes the administrator password for all our PCs and servers, which is shared by the Operations Manager and may be available to our Computer Service Company (see Roles And Responsibilities).

We discourage co-workers from sharing their passwords, but we accept the reality that co-workers will often learn one another's passwords. Therefore, the ISM changes all workstation passwords at least once a year and whenever an employee leaves.

The workstation administrator password is often stored by multiple programs, including the backup system. Changing it everywhere is a major undertaking, so we do it only when security urgently requires it, such as when a senior staff person leaves on bad terms.

No Unencrypted Sensitive Information

We do not keep personal information on laptops, or other handheld or portable devices. We store backups on mirrored hard drives on our server, encrypted with Strong Passwords using Strong Encryption.

Network Security

We configure our network as follows:

- Firewall passes GRC test.
- Passwords changed when staff leaves. Workstation passwords changed annually.
- Cabling secure.
- We do not employ a wireless network.
- Strong Passwords, multiple lockout.
- Antivirus (Sophos) kept up to date both in version and in signatures and certified by ICSA.
- Malware software kept up to date.
- ISM performs scan in case of slowness or another anomaly with workstation performance.
- Anti-phishing and poisoned website measures administered by antivirus software (Sophos).
- Remote access is only by remote access software that is encrypted and secure, using screen blanking and keyboard locking.

Computer Security

When a new computer is added to our network, it is secured with our master administrator password, and users are given appropriate logins with passwords. These passwords, like all passwords in the company, are kept on the Master Password list. If a hard drive is unable to be erased because it is broken, we destroy its electrical leads and send it to our secure offsite destruction facility.

When a Staff Person Leaves Our Organization

When a staff person leaves our organization, all passwords that person used are changed, so that the person no longer has access to our computer network remotely or if s/he visits the office. The person also returns any keys used to physically secure personal information.

If a Breach Occurs

If our ISM determines that PI has been stolen, she will notify the Office of Consumer Affairs & Business Regulation (OCABR) and the Attorney General's Office, describing the theft in detail, and work with authorities to investigate the crime and to protect the victim's identity and credit. To the extent possible, our ISM will also warn the victims of the theft so that they can protect their credit and identity.

Computer Security:

- Everyone must enter a correct username-password pair to access one of our computers.
- Operating System set to automatically download security updates with ISM approval for installation.
- Antivirus (Sophos) configured to download and install both code and virus signature updates.
- Malware software is configured to automatically download and install security updates. If computers seem to be slow or otherwise not working normally, the ISM runs scans on the computer. If the problem persists, the ISM contacts AKUITY Technologies. for assistance.
- Anti-phishing and poisoned website measures (Sophos).
- Remote access is only by remote access software that is encrypted and secure, using screen blanking and keyboard locking.

Our computers are on a Secure Network

The firewall passes the GRC test.

When a staff member leaves, the Information Security Manager removes or changes all passwords to which that person had access.

Each year, the Information Security Manager changes all workstation passwords.

Network cables are secure.

Roles and Responsibilities

Role Name	Responsibility	Person
Owner	General Control, Direction and Supervision	Jack Gottlieb & Kevin Adolph
Operations Manager	All responsibilities assigned by the Owner, associated with the day to day operation of the business.	Cindy Meisenheimer
Information Security Manager	Regularly review and update this Information Security Plan; train new staff and refresh training of all staff on information security; regularly audit staff and vendor on information security compliance.	Kevin Adolph
Assistant Operations Manager	Day to day supervision of all warehouse activity, distribution of payroll, purchasing, supervision of office activity in the absence of the Operations Manager.	Lei Foster
Office Manager	Accounts payable and receivable, payroll, health benefit administration, office management and organization.	Cindy Meisenheimer
Warehouse Staff	Storage and transport of boxed records, bins, folders and files.	Various
Computer Service Company	Install and repair computers and software. Consult on issues relating to computers or security.	AKUITY Technologies
CPA Firm	Audit financial records and advise on financial issues.	Brennan & Bustin
Legal Counsel	Advise and represent in legal matters.	Seder & Chandler
Payroll Service	Issue payroll as directed by the Operations Manager and Office Manager.	Intuit

Name Date

201 CMR 17.00 COMPLIANCE CHECKLIST

The Office of Consumer Affairs and Business Regulation has compiled this checklist to help small businesses in their effort to comply with 201 CMR 17.00. **This Checklist is not a substitute for compliance with 201 CMR 17.00.** Rather, it is designed as a useful tool to aid in the development of a written information security program for a small business or individual that handles "personal information." Each item, presented in question form, highlights a feature of 201 CMR 17.00 that will require proactive attention in order for a plan to be compliant.

The Comprehensive Written Information Security Program (WISP)

- q Do you have a comprehensive, written information security program ("WISP") applicable to all records containing personal information about a resident of the Commonwealth of Massachusetts ("PI")?
- q Does the WISP include administrative, technical, and physical safeguards for PI protection?
- q Have you designated one or more employees to maintain and supervise WISP implementation and performance?
- q Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices that contain personal information?
- q Have you chosen, as an alternative, to treat all your records as if they all contained PI?
- q Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?
- q Have you evaluated the effectiveness of current safeguards?
- q Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?
- q Does the WISP include disciplinary measures for violators?
- q Does the WISP include policies and procedures for when and how records containing PI should be kept, accessed or transported off your business premises?
- q Does the WISP provide for immediately blocking terminated employees

- q Is the length of time that you are storing records containing PI limited to the time reasonably necessary to accomplish your legitimate business purpose or to comply with state or federal regulations?

- q Is access to PI records limited to those persons who have a „need to know in connection with your legitimate business purpose, or in order to comply with state or federal regulations?

- q In your WISP, have you specified the manner in which physical access to PI records is to be restricted?

- q Have you stored your records and data containing PI in locked facilities, storage areas or containers?

- q Have you instituted a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary?

- q Are your security measures reviewed at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PI records?

- q Do you have in place a procedure for documenting any actions taken in connection with any breach of security; and does that procedure require post-incident review of events and actions taken to improve security?

Additional Requirements for Electronic Records

- q Do you have in place secure authentication protocols that provide for:

- q Control of user IDs and other identifiers?

    - o A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)?
    - o Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect?
    - o Restricting access to PI to active users and active user accounts?
    - o Blocking access after multiple unsuccessful attempts to gain access?

- q Do you have secure access control measures that restrict access, on a need-to-know basis, to PI records and files?

- q Do you assign unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls?

- q Do you, to the extent technically feasible, encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly?

- q Do you, to the extent technically feasible, encrypt all PI stored on laptops or other portable devices?

- q Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?

- q On any system that is connected to the Internet, do you have reasonably up-to-date firewall protection for files containing PI; and operating system security patches to maintain the integrity of the PI?

- q Do you have reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions?

- q Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?