2011

Data Security and Privacy Toolkit

NATIONAL ASSOCIATION *of* REALTORS®

Table of Contents

Introduction

Trust is at the heart of the real estate business. In this digital economy, trust has taken on new dimensions that impact how real estate professionals collect, share and, most importantly, protect the information they use in their businesses. Creating a data security program for your business means implementing and maintaining reasonable safeguards to protect the security, confidentiality, and integrity of data, including proper disposal of the data. A privacy policy is a document that discloses some or all of the ways your business collects, shares, protects, and destroys personal information. Often, a written data security program is an internal document provided to and implemented by employees, whereas a privacy policy is distributed more widely, such as on your organization's website.

This Data Security and Privacy Toolkit aims to educate real estate associations, brokers, agents, and multiple listing services about the need for data security and privacy; and to assist them in complying with legal responsibilities. The Toolkit provides information about state laws and pending federal regulations regarding data security and privacy protection that may affect your business.In regards to compliance, the Toolkit includes various checklists of issues to consider when drafting a security program tailored to your business's needs. There is no one-size-fits-all approach to security and compliance, but the NATIONAL ASSOCIATION OF REALTORS® (NAR) aims to provide your real estate business with the tools necessary for developing a program that best suits your business. In addition, the Toolkit contains reference to guidance and sample policies created by government or other organizations. The Federal Trade Commission (FTC) has promoted five key principles for protecting personal information. This Toolkit adheres closely to those key principles, which are further explained and set forth in the FTC publication, "Protecting Personal Information; A Guide for Business."[1]

[1] Federal Trade Commission, "Protecting Personal Information; A Guide for Business," available at: http://www.ftc.gov/infosecurity/.

The Importance of Data Security and Privacy

The first question you may ask yourself is: "Why should I care?" Whether you realize it or not, most real estate businesses — associations, brokerages, and MLSs — keep sensitive, personal information in their files. Associations may collect members' credit card or bank account information in relation to payments for educational courses, RPAC contributions, or other goods and services. Also, associations are employers, so they may also maintain Social Security numbers and health information of their employees.

Brokers and their agents collect personal information for a variety of reasons. They may collect:

- Social Security numbers in order to perform credit checks on renters or to complete a short sale transaction;
- Bank account information and Social Security numbers contained in mortgage documents and closing statements;
- Personal checks given as earnest money;
- Credit card information to make various payments for inspections or appraisals; or
- Driver's license numbers as a safety precaution when agents leave the office with a new client for the first time.

Oftentimes, this personal information is collected because the agent is trying to be helpful to his client. But, in reality, the agent may be helping himself and his broker to some legal risk.

If personal information falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Businesses may also be concerned about reputational harm. State legislatures realized the potential for this harm and have enacted laws to help protect consumers' personal information. Given the cost of a security breach, safeguarding personal information is just plain good business.

Know the Laws

It is important for you to know the laws regarding data security and privacy that affect your organization. The purpose of most data security regulation is to encourage businesses to protect personal information under their control in order to avoid misappropriation of that information. Some states have enacted laws that require businesses to have a written information security program in place, dispose of personal information that serves no business purpose, and notify individuals when their personal information may have been accessed because of a security breach. Most state and pending federal legislation allows businesses to take a reasonableness approach to implementing a security program by taking into account the particular business' size, scope of business, amount of resources, and nature and quality of data collected or stored.

Currently, there are no federal laws regarding data privacy that specifically apply to real estate associations or brokerages. However, the Gramm-Leach-Bliley Financial Modernization Act applies to businesses that qualify as financial institutions pursuant to the Act.[2] Some associations and brokerages may also be subject to the Identity Theft Red Flags and Address Discrepancy Rules (Red Flags Rules) contained in the Fair and Accurate Credit Transactions Act of 2003 (FACTA).[3] The Red Flags Rules require all creditors, and those who regularly arrange for credit to be provided, to establish policies and procedures to protect against identity theft. Although the Red Flags Rules became effective on January 1, 2008, the mandatory compliance date has been delayed several times and now is scheduled for December 31, 2010. Although a comprehensive, federal data security law does not exist right now, several federal bills that address data security and privacy have been proposed and debated in Congress and legislation may be forthcoming. These bills contain many elements commonly found in existing state laws, so compliance with state laws should be a good step toward compliance with any future federal legislation.

The National Conference of State Legislatures (NCSL) maintains a list of state data security and privacy laws and pending legislation. This website is an extremely helpful resource to determine which states maintain such laws and where those laws are codified. According to NCSL, 29 states have some type of law regarding the proper disposal of personal information[4] and 46 states, D.C., Puerto Rico, and the Virgin Islands have laws regarding notification requirements in the event of a security breach.[5] Review the charts on the following pages to see if your state is listed. Also, keep in mind that many state laws, such as Massachusetts, pertain to any business in the country that maintains personal information of a resident of that state. So, it is wise not only to refer to the laws of the state in which your business is located, but also the laws of the states where the individuals whose personal information you collect reside.

The various state laws regarding data security have many common elements, but some differences as well. For example, each state has its own definition of "personal information." In Massachusetts, "personal information" is defined as:

> *A resident's first name and last name (or first initial and last name) in combination with any one or more of the following data elements that relate to such resident:*
>
> *(a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number (or credit or debit card number) with or without any required security code, access code, personal ID number, or password that would permit access to a resident's financial account.*[6]

[2] Gramm-Leach-Bliley Financial Modernization Act (P.L. 106-102, 113 Stat. 1338) (1999). This Data Security and Privacy Toolkit was created without reference to the Gramm-Leach-Bliley Financial Modernization Act and should not be relied upon for compliance with that Act.

[3] Fair and Accurate Credit Transactions Act of 2003; Pub. Law 108-159 (Dec. 4, 2003); 117 Stat. 1952. To learn more about the Red Flags Rules and how it may affect your organization, check out "Questions and Answers About the Identity Theft Red Flag Requirements" created by the NATIONAL ASSOCIATION OF REALTORS®, available at: http://www.realtor.org/wps/wcm/connect/7ef33f004af68a5f96baf7e7df25f375/govaff_factact_idtheft2.pdf?MOD=AJPERES&CACHEID=7ef33f004af68a5f96baf7e7df25f375.

[4] National Conference of State Legislatures, "Data Disposal Laws," available at: http://www.ncsl.org/default.aspx?tabid=21075.

[5] National Conference of State Legislatures, "State Security Breach Notification Laws," available at: http://www.ncsl.org/default.aspx?tabid=13489.

[6] Standards for the Protection of Personal Information of Residents of the Commonwealth; 201 CMR § 17.02.

Know the Laws (continued)

California's definition of "personal information" is similar, but slightly different as it is defined as:

> *An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:*
>
> *(1) Social Security number; (2) Driver's license number or CA ID card number; (3) Account number, credit card, or debit card number; in each case, in combination with any required security code, access code, or password that would permit access to an individual's account; (4) Medical information; (5) Health insurance information.*[7]

The two definitions above may look similar, but their difference is significant. The Massachusetts definition appears to be broader because it doesn't matter whether or not the data elements are encrypted. Information is encrypted if the data is transformed in a way that its meaning cannot be ascertained or understood without the use of a confidential process or key. Also, in Massachusetts, a financial account number need not be accompanied by a security code or password. In California, the statute would not be triggered if one of the data elements was encrypted and, in order to qualify as "personal information," an account number must be found in combination with a security code or password.

Unless otherwise noted, for the purpose of this Toolkit, "personal information" will be interpreted broadly to mean any information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.[8] In regards to compliance, it is necessary for businesses to consult applicable law and advisable to consult legal counsel.

[7] Cal. Civ. Code § 1798.82(e).

[8] See definition of "Personally Identifiable Information" at: http://en.wikipedia.org/wiki/Personally_identifiable_information.

DATA DISPOSAL LAWS

Personal identifying information is often collected by businesses and stored in various formats, both digital and traditional paper. With identity theft a growing problem in the country, many states have passed laws that require entities to destroy, dispose, or otherwise make personal information unreadable or undecipherable, in order to protect an individual's privacy. At least 29 states, listed below, provide laws that govern the disposal of personal data held by businesses and/or government.

As of August 18, 2010

Alaska	Alaska Stat. § 45.48.500
Arizona	Ariz. Rev. Stat. § 44-7601
Arkansas	Ark. Code Ann. § 4-110-104
California	Cal. Civ. Code § 1798.81
Colorado	Colo. Rev. Stat. § 6-1-713
Connecticut	Conn. Gen. Stat. Ann. § 42-471
Georgia	Ga. Code § 10-15-2
Hawaii	Haw. Rev. Stat. § 487R-2
Illinois	20 ILCS 450/20
Indiana	Ind. Code § 24-4-14-8
Kansas	Kan. Stat. Ann. § 50-7a03
Kentucky	Ky. Rev. Stat. § 365.725
Massachusetts	Mass. Gen. Laws Ch. 93I, § 2
Maryland	Md. Code, Comm. Law § 14-3507
Michigan	MCL § 445.72a
Missouri	Mo. Stat. § 288.360
Montana	Mont. Code Ann. § 30-14-1703
Nevada	Nev. Rev. Stat. § 603A.200
New Jersey	N.J. Stat. § 56:8-162
New York	N.Y. Gen. Bus. Law § 399-H
North Carolina	N.C. Gen. Stat. § 75-64
Oregon	Ore. Rev. Stat. § 646A.622
Rhode Island	R.I. Gen. Laws § 6-52-2
South Carolina	S.C. Code § 37-20-190
Texas	Tex. Bus. & Com. Code. Ann. § 72.004
Utah	Utah Code Ann. § 13-44-201
Vermont	9 Vt. Stat. Ann. § 2445
Washington	Wash. Rev. Code § 19.215.020
Wisconsin	Wisc. Stat. § 134.97

PLEASE NOTE: The National Conference of State Legislatures serves state legislators and their staff. This site provides comparative information only and should not be construed as legal advice.

STATE SECURITY BREACH NOTIFICATION LAWS

Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. States with no security breach law: Alabama, Kentucky, New Mexico, and South Dakota.

As of April 12, 2010

Alaska	Alaska Stat. § 45.48.010 et seq.
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 et seq.
California	Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. 36a-701(b)
Delaware	Del. Code tit. 6, § 12B-101 et seq.
Florida	Fla. Stat. § 817.5681
Georgia	Ga. Code §§ 10-1-910, -911
Hawaii	Haw. Rev. Stat. § 487N-2
Idaho	Idaho Code §§ 28-51-104 to 28-51-107, 2010 H.B. 566
Illinois	815 ILCS 530/1 et seq.
Indiana	Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq., 2009 H.B. 1121
Iowa	Iowa Code § 715C.1 (2008 S.F. 2308)
Kansas	Kan. Stat. 50-7a01, 50-7a02
Louisiana	La. Rev. Stat. § 51:3071 et seq.
Maine	Me. Rev. Stat. tit. 10 §§ 1347 et seq., 2009 Public Law 161
Maryland	Md. Code, Com. Law § 14-3501 et seq.
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.
Michigan	Mich. Comp. Laws § 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	2010 H.B. 583 (effective July 1, 2011)
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code § 30-14-1701 et seq., 2009 H.B. 155, Chapter 163
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807
Nevada	Nev. Rev. Stat. 603A.010 et seq.
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21
New Jersey	N.J. Stat. 56:8-163
New York	N.Y. Gen. Bus. Law § 899-aa
North Carolina	N.C. Gen. Stat § 75-65
North Dakota	N.D. Cent. Code § 51-30-01 et seq.
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. § 74-3113.1 and 2008 H.B. 2245
Oregon	Oregon Rev. Stat. § 646A.600 et seq.
Pennsylvania	73 Pa. Stat. § 2303
Rhode Island	R.I. Gen. Laws § 11-49.2-1 et seq.
South Carolina	S.C. Code § 39-1-90
Tennessee	Tenn. Code § 47-18-2107, 2010 S.B. 2793
Texas	Tex. Bus. & Com. Code § 521.03
Utah	Utah Code §§ 13-44-101, -102, -201, -202, -310
Vermont	Vt. Stat. tit. 9 § 2430 et seq.
Virginia	Va. Code § 18.2-186.6, 2010 H.B. 1039 (effective January 1, 2011)
Washington	Wash. Rev. Code § 19.255.010, 2010 H.B. 1149 (effective July 1, 2010)
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98 et seq.
Wyoming	Wyo. Stat. § 40-12-501 to -502
District of Columbia	D.C. Code § 28- 3851 et seq.
Puerto Rico	10 Laws of Puerto Rico § 4051 et. seq.
Virgin Islands	V.I. Code § 2208

PLEASE NOTE: The National Conference of State Legislatures serves state legislators and their staff. This site provides comparative information only and should not be construed as legal advice.

FTC: Five Key Principles to a Sound Data Security Program

The Federal Trade Commission has set forth the following five key principles for businesses to follow when creating a data security program.[9]

1 *Take stock.*
Know what personal information you have in your files and on your computers.

2 *Scale down.*
Keep only what you need for your business.

3 *Lock it.*
Protect the information that you keep.

4 *Pitch it.*
Properly dispose of what you no longer need.

5 *Plan ahead.*
Create a plan to respond to security incidents.

This Toolkit follows the FTC's principles and provides your real estate business with tools for implementing a data security program that best suits your organization.

[9] Federal Trade Commission, "Protecting Personal Information; A Guide for Business," available at: http://www.ftc.gov/infosecurity/.

Take Stock

Perform an information inventory to discover what type of information your business maintains and why; who maintains or has access to the collected information; how the information is collected; and whether a user or consumer may opt-out of your collection of the information. The more thorough your inventory, the better equipped you'll be when creating the written data security program and the better protected your organization will be.

In order to track what information your business is collecting, talk to representatives in your information technology staff, human resources office, accounting personnel, outside service providers, and independent contractors. Association executives and brokers should also inventory all computers, laptops, flash drives, disks, home computers, mobile devices, and other equipment to find out where sensitive data is stored.

INFORMATION INVENTORY CHECKLIST

A complete information inventory should seek answers for the following questions. Possible answers are provided as examples only.

☐ **Who sends personal information to your business?**
- ○ Consumers
- ○ Independent contractors
- ○ Employees
- ○ Members
- ○ Credit card companies
- ○ Banks or other financial institutions
- ○ Brokerages
- ○ Call centers
- ○ Contractors

☐ **How does your business receive personal information?**
- ○ Websites
- ○ E-mails
- ○ Mail
- ○ Interviews
- ○ Cash registers

☐ **Where does your business keep the information you collect at each entry point?**
- ○ Central computer database
- ○ Individual laptops
- ○ Disks
- ○ File cabinets
- ○ Branch offices
- ○ Employees/licensees have files at home
- ○ Mobile devices

☐ **Who has — or could have — access to the information?**
- ○ Specific employees/licensees
- ○ Vendors
- ○ Independent contractors
- ○ Consumers
- ○ Public

☐ **What kind of information does your business collect at each entry point?**
- ○ Individuals' first names or initials and last names
- ○ Postal address
- ○ Telephone/fax number
- ○ E-mail address
- ○ Social Security number
- ○ Driver's license number
- ○ Tax ID
- ○ Passport number
- ○ Real Estate License number
- ○ Other Government-issued identification number
- ○ Credit card or debit card number
- ○ Checking account information
- ○ Security code, access code, or password for an individual's financial account
- ○ Credit history
- ○ Mortgage application
- ○ Medical information
- ○ Health insurance information
- ○ Race/ethnicity
- ○ Religious belief
- ○ Sexual orientation
- ○ Financial information (e.g., balance, history, etc.)
- ○ Precise geolocation information
- ○ Unique biometric data
- ○ Website user activity on the website
- ○ Unique persistent identifier (e.g., customer number, user alias, IP address, etc.)
- ○ Preference profile (e.g., a list of information, categories, or information or preferences associated with a specific individual or computer or device)

Scale Down

Once you've performed an information inventory and understand what type of information your business collects and how and why, it's time to consider whether or not you need to continue collecting or retaining such information. Here's the rule:

> *If your association or brokerage does not have a legitimate business need for the personally identifying information—then don't collect it. If there is a legitimate business need for the information, then keep it only as long as it's necessary. Once that business need is over, then properly dispose of it.*

If you must keep information for business reasons or to comply with the law, then develop and adhere to a document retention policy to identify what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when you no longer need it. Refer to the tips for creating a Document Retention Policy provided in the section titled "Pitch It."

If your association or brokerage must collect credit card information, the FTC offers a few tips for maintaining security:

- Only print the truncated credit or debit card number on consumer receipts and do not include the card's expiration date.
- Don't retain the credit card account number or expiration date unless you have an essential business need to do so.
- Check the default settings on your software that reads credit card numbers and processes the transactions. Sometimes it's preset to keep information permanently, so change the default setting to make sure you're not keeping information you don't need.[10]

[10] Federal Trade Commission, "Protecting Personal Information; A Guide for Business," available at: http://www.ftc.gov/infosecurity/.

Lock It

Now you've taken stock and know what personal information your organization collects, how it is collected, and why. You've scaled down, and know what personal information is necessary for you to continue collecting and what information you can avoid collecting in the future. Now it's time for you to protect the personal information you maintain. The FTC recommends four key elements for your protection plan: physical security, electronic security, employee training, and the security practices of contractors and service providers.

CHECKLIST FOR PROTECTING PERSONAL INFORMATION

The following checklist contains tips and recommendations for protecting personal information. For more guidance on protecting personal information, check out the FTC's plain-language, interactive tutorial at **www.ftc.gov/infosecurity**.

☐ Physical Security

- ○ Store paper documents and tangible files containing personally identifiable information in a locked room or in a locked file cabinet.
- ○ Limit access to employees with a legitimate business need.
- ○ Require employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- ○ If you maintain offsite storage facilities, limit employee access to those with a legitimate business need.

☐ Electronic Security

- ○ Identify the computers or servers where personally identifiable information is stored.
- ○ Identify all connections to those computers. For example, the Internet, electronic cash register, computers at branch offices, computers used by service providers to support your network, and wireless devices.
- ○ Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
- ○ Don't store personally identifiable information on any computer with an Internet connection unless it's essential for conducting your business.
- ○ Encrypt sensitive information that you send to third parties over public networks.
- ○ Regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on servers on your network.
- ○ When you receive or transmit credit card information or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.
- ○ Pay particular attention to the security of your Web applications—the software used to give information to visitors to your website and to retrieve information from them.
- ○ Require the use of a token, smart card, thumb print, or other biometric—as well as a password—to access a computer that contains personal information.
- ○ Password Management
  - Require employees to use strong passwords. The longer the password the better. Mix letters, numbers, and characters.
  - Prohibit sharing or posting passwords.
  - Use password-activated screen savers to lock employee computers after a period of inactivity.
  - Warn employees about social engineering. For example, alert them to possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.
  - When installing new software, immediately change vendor-supplied default passwords to a more secure, strong password.
- ○ Laptop Security
  - Assess whether personal information really needs to be stored on a laptop. If not, wipe it out.
  - If a laptop contains personal information, encrypt it and configure it so users can't download any software or change the security settings without approval from your IT specialist.
  - Train employees to be mindful of security when they're on the road.
- ○ Firewalls
  - Use a firewall to protect your computer from hacker attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.
  - Set access controls—settings that determine who gets through the firewall and what they will be allowed to see—to allow only trusted employees with a legitimate business need to access the network.
- ○ Wireless and Remote Access
  - Determine if you use wireless devices like cell phones to connect to your computer network or to transmit personal information.
  - Consider using encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases.

Lock It (continued)

CHECKLIST FOR PROTECTING PERSONAL INFORMATION (continued)

- ○ Detecting Breaches
  - Consider using an intrusion detection system to detect network breaches when they occur.
  - Maintain central log files of security-related information to monitor activity on your network so that you can spot and respond to attacks.
  - Monitor incoming traffic for signs that someone is trying to hack in.
  - Monitor outgoing traffic for signs of a data breach.

☐ Employee Training

- ○ A data security program is only as strong as the employees who implement it.
- ○ Check references or do background checks before hiring employees who will have access to personal data.
- ○ Make sure employees and independent contractors understand that abiding by your company's data security program is an essential part of their duties.
- ○ Require employees to notify you immediately if there is a potential security breach, such as a lost or stolen laptop or a downloaded virus.
- ○ Know which employees have access to personal information.
- ○ Have a procedure in place for making sure that workers who leave your employ no longer have access to personal information.
- ○ Impose disciplinary measures for security policy violations.

☐ Security Practices of Contractors and Service Providers

- ○ Before you outsource any of your business functions — payroll, Web hosting, customer call center operations, cloud computing, or the like — investigate the company's data security practices and compare their standards to yours.
- ○ Insist that your service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of data.
- ○ Insist that contractors and service providers adhere to all applicable federal and state laws regarding data security and privacy.

Pitch It

According to the FTC and many state laws, proper disposal of personal information is an important step in any data security program. Implementation of a Document Retention Policy that is reasonable and appropriate will help prevent unauthorized access to personal information. But the question remains: what constitutes "proper disposal"? In general, personal information is properly disposed if it cannot be read or reconstructed. The FTC recommends that a business burn, shred, or pulverize paper records and use wipe utility programs or otherwise destroy electronic records. Simply deleting files from the computer using the keyboard or mouse commands usually isn't sufficient. Also, make sure employees who work from home follow the same procedures for disposing of personal information.

Like all data security policies, there is no "one-size-fits-all" model for document retention. NAR has created a "Checklist for Creating a Document Retention Policy."[11]

The following checklist provides a brief description of the process an association or brokerage should undertake in creating a Document Retention Policy. Following that is a list of different types of documents and some recommended timeframes for how long the association or brokerage should maintain these records. This checklist is not intended to be comprehensive or even authoritative; rather, it is intended to serve as a guide for associations and brokerages in creating their own policies. State law will determine how long an organization needs to maintain its records. Remember, a Document Retention Policy adopted and followed by the association or brokerage will likely reduce the costs and burdens of any future litigation.

[11] The "Checklist for Creating a REALTOR® Association Record Retention Policy" was developed in 2009 and is available on the Law & Policy page of *REALTOR.org* at: http://www.realtor.org/letterlw.nsf/pages/0307recordpolicy?OpenDocument&Login.

CHECKLIST FOR CREATING A DOCUMENT RETENTION POLICY

A. Process for Creating a Document Retention Policy

1. **IDENTIFY SOURCES AND TYPES OF INFORMATION.**
   Gather together the employees who are familiar with the documents and other information your business maintains. Depending on the size of the organization, the number of individuals could vary. A person familiar with how the business maintains electronic information should attend the meeting. Please refer to the "Take Stock" section regarding information inventory for more information and guidance for completing this step.

2. **IDENTIFY AND DOCUMENT CURRENT RETENTION POLICIES.**
   Determine what policies (if any) are currently governing your organization's document retention policies and reduce those to writing, including its policies for retaining electronic information.

3. **EVALUATE EXISTING POLICIES.**
   Decide whether your organization's current policies are adequate or whether a new policy is necessary.

4. **CREATE A POLICY.**
   The Document Retention Policy should include the following:
   - How long certain documents should be retained
   - Policy's effective date and date of last review
   - Individual responsible for the policy
   - Purpose of the policy
   - Definitions (if needed)
   - Process for preserving records if litigation arises or is likely

5. **LEGAL REVIEW OF DOCUMENT RETENTION POLICY.**
   Once the policy is created, have it revised by your legal counsel. You may choose to involve an attorney at the fourth stage during the crafting of the policy.

6. **DISTRIBUTE THE POLICY TO EMPLOYEES AND INDEPENDENT CONTRACTORS AND MAKE SURE THAT THE POLICY IS BEING FOLLOWED.**
   This is the most important step! Having a policy that isn't followed will actually be worse than not having any policy if litigation arises.

7. **PLAN TO PERIODICALLY REVIEW THE POLICY TO MAKE SURE IT IS STILL RELEVANT.**
   Set a date in the future to assess the policy.

Pitch It (continued)

CHECKLIST FOR CREATING A DOCUMENT RETENTION POLICY (continued)

B. Issues to Consider When Creating a Document Retention Policy

A number of issues will arise during the creation of a Document Retention Policy. A few are listed below:

FORMAT USED TO MAINTAIN DOCUMENTS.
Generally, there are no requirements on the type of format that must be used to maintain documents and other information. Reducing paper documents to an electronic format will save physical space, but could present problems if litigation arises. To avoid these problems, all electronic documents should be stored in a read-only format or other unalterable format in order to demonstrate that the documents are in their original state.

PRIVACY CONSIDERATIONS AND PROPER DOCUMENT DESTRUCTION.
Certain types of records, such as employment records, are governed by state or federal privacy laws. Therefore, you must be familiar with those laws and also any rules or other restrictions governing the destruction of these documents.

OTHER LEGAL CONSIDERATIONS.
The legal requirements for each company will vary based on a variety of factors. For example, certain employment statutes require minimum numbers of employees in the workplace before they apply to a business owner. IRS audits are generally initiated within three years, but the IRS can audit a return seven years later if negligence was involved and indefinitely in cases of tax fraud. Each company must be aware of the laws that apply to their situation.

C. Creating a Document Retention Policy

Below is a list of types of documents that you may maintain in their files. Next to each entry are some suggested time periods for which the organization should maintain these documents. These are conservative estimates, and do not prevent any organization from extending these time periods beyond these minimums. These requirements vary by state, and so you will need to consult with your attorney when creating the policy, as stated above.

ACCOUNTING RECORDS
- Accounts payable (seven years)
- Accounts receivable (seven years)
- Annual financial statements (permanent)
- Bank statements (seven years)
- Bank reconciliations (seven years)
- Canceled checks: routine matters (seven years)
- Canceled checks: special (loan repayment, etc.) (permanent)
- Correspondence: routine (four years)
- Deeds and closing papers (permanent)
- Deposit slips (four years)
- Electronic payment records (seven years)
- Employee expense reports (seven years)
- Fixed-asset acquisition invoices (after disposal) (seven years)
- Freight bills (seven years)
- General ledgers (permanent)
- Income tax returns (permanent)
- Inventory count & costing sheets (seven years)
- Insurance policies (after expiration) (four years)
- Investments (after disposal) (seven years)
- Mortgages, loans & leases (paid) (seven years)
- Payroll journals & ledgers (permanent)
- Purchase orders (except accounts payable copy) (one year)
- Purchase invoices & orders (seven years)
- Receiving sheets (two years)
- Sales commission reports (five years)
- Sales records (seven years)
- Sales tax returns & exemption support (five years)
- Subsidiary ledgers (seven years)
- Tax returns (federal & state) (if applicable) (permanent)
- Trial balances (permanent)

CORPORATE RECORDS
- Articles of Incorporation and amendments (permanent)
- Bylaws and amendments (permanent)
- Corporate filings (permanent)
- Corporate Minute Book (permanent)
- IRS Exemption Letter (permanent)

ELECTRONICALLY STORED INFORMATION
Specific documents in electronic formats will be treated according to the timeframes set forth elsewhere in the policy. The policy should state how long an organization maintains information stored on its backup tapes and other backup systems. The policy should also state that the purpose of the backups is to restore the business's computer network in the event of a crash.

EMPLOYMENT RECORDS
- Documents relating to job recruitment: advertising, job orders submitted to employment agencies, interviewing, testing, hiring, training, demotions, promotions, layoffs, discharge, and other personnel decisions (one year)
- Employee benefit plan documents (duration of plan)
- Garnishments/wage assignments (three years)
- Immigration I-9 forms (duration of employment plus one year, minimum of three years)
- Medical records relating to the exposure of the employee to any toxic or hazardous substances (duration of employment plus 30 years)
- Payroll records showing name, address, date of birth, occupation, rate of pay, and weekly compensation (three years)
- Personnel records (ten years after employment ends)
- Record of all occupational injuries, including those under state worker's compensation law and any ERISA awards (five years for ERISA; state law requirements will vary)

LEGAL DOCUMENTS
- Contracts (ten years after expiration)
- License Applications (one year after expiration)
- Licenses (one year after expiration)
- Trademarks, Patents & Copyrights (permanent)
- Warranties & Guaranties (two years beyond terms of the warranty)
- Correspondence: legal (permanent)

MLS DOCUMENTS
- Rules and Regulations (permanent)
- MLS Policies (permanent)
- Listing agreements (at least until expiration of listing)
- Sold property information (ten years)
- Lockbox key agreements/leases (one year after agreement terminates)
- MLS Service Mark License Agreements (Permanent)
- Contracts (ten years after expiration)
- Subscription Agreements (ten years after expiration)
- Participation Agreements (ten years after expiration)
- Website Click-Through Confirmations (ten years)

ASSOCIATION DOCUMENTS
- Association charter (permanent)
- Territorial jurisdiction (permanent)
- Member file & membership applications (two years after membership terminates, with Social Security number and other financial information removed (if applicable))
- Professional Standards Hearing Records: Ethics (result of hearing — permanent; rest of hearing file — minimum of one year after satisfaction of sanctions (if any) and there is no threat of litigation)
- Arbitration/Mediation (minimum of one year after payment of award (if any) and there is no threat of litigation)

PROPERTY RECORDS
- Deeds of Title (permanent)
- Leases (two years after expiration)
- Depreciation schedules (permanent)
- Property Damage (seven years)
- Property Tax (permanent)
- Appraisals (permanent)
- Blueprints/Plans (permanent)
- Warranties & Guaranties (two years beyond terms of the warranty)

PENSION & PROFIT SHARING
- ERISA disclosure documents (six years from date disclosure was due)
- IRS Determination Letter(s) (permanent)
- Forms 5500 & plan documents (permanent)

Plan Ahead

As explained in the Introduction, currently many states have laws that require a business to keep personal information secure and to notify individuals in the event that security is breached. Therefore, it is advisable and may be necessary to have a written data security program in place and a policy that addresses what to do in the event of a breach. Remember, your organization may be subject to the laws of multiple states if it collects personal information from residents of multiple states. So, it is important to know which laws you must adhere to.

Although each state data security and breach notification law is different, they contain some common elements. For example, many laws require businesses to designate an employee to coordinate and implement the data security and breach notification program. Such laws also set forth the definition of "personal information" and the requirements of breach notification, such as who must receive notification and the timing, format, and content of such notification. Most laws also include provisions regarding a business's liability for failure to comply. In addition to other fines and penalties, at least ten state laws include a private right of action to allow individuals to sue businesses for actual damages that might result from not receiving timely notice of a security breach.[12]

This section of the Toolkit provides information to help in the implementation of your own written data security program and includes the following:

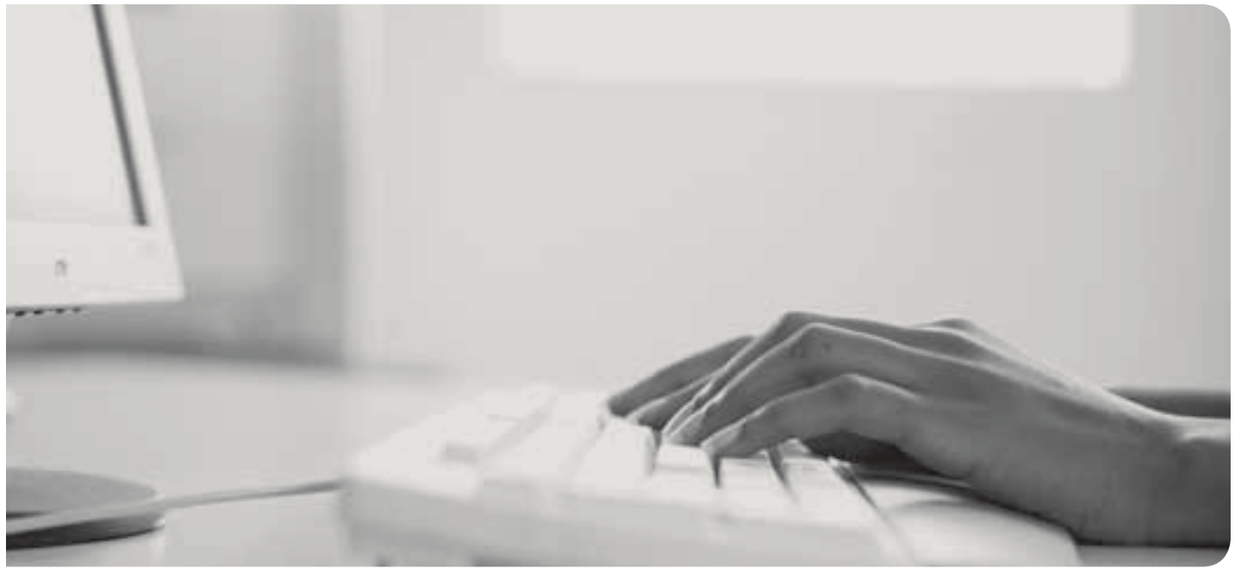
- Checklist for implementing a data security program
- Model written data security program created by the Massachusetts Association of REALTORS®
- Checklist for responding to a data security breach
- Sample breach notification correspondence

For additional guidance, check out the sample written security program and checklist created by the Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation.[13]

Please remember that the information contained herein is not intended to be comprehensive or even authoritative; rather, it is intended to serve as a guide for real estate businesses in creating their own policies.

[12] Practical Law Journal, "Privacy and Data Security Toolkit," April 2010.

[13] Commonwealth of Massachusetts, Office of Consumer Affairs and Business Regulation, "A Small Business Guide: Formulating a Comprehensive Written Information Security Program," available at: http://www.mass.gov/Eoca/docs/idtheft/sec_plan_smallbiz_guide.pdf; and "201 CMR 17.00 Compliance Checklist," available at: http://www.mass.gov/Eoca/docs/idtheft/compliance_checklist.pdf.



CHECKLIST FOR IMPLEMENTING A DATA SECURITY PROGRAM

- ☐ Designate one or more employees to maintain the data security program.
- ☐ Understand and describe in writing your organization's current safeguards for limiting risks to the security or integrity of any personal information including but not limited to:
  - ○ Ongoing employee training
  - ○ Employee compliance with policies and procedures
  - ○ Means for detecting and preventing security system failures
- ☐ Implement reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas, or containers.
- ☐ Implement reasonable restrictions upon how personal information is stored, accessed, and transported by employees and independent contractors outside of business premises.
- ☐ Impose disciplinary measures for violations of the data security program.
- ☐ Prevent terminated employees from accessing records containing personal information.
- ☐ Oversee service providers, by:
  - ○ Choosing service providers carefully
  - ○ Requiring third-party service providers by contract to implement and maintain such appropriate security measures for personal information
- ☐ Regularly monitor the effectiveness of the data security program and upgrade information safeguards as necessary to limit risks.
- ☐ Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- ☐ Document responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.
- ☐ Provide for secure user authentication protocols and access control measures.
- ☐ Encrypt all transmitted records and files containing personal information that will travel across public networks, be transmitted wirelessly, or are stored on laptops or other portable devices.
- ☐ Implement reasonable monitoring of systems for unauthorized use of or access to personal information.
- ☐ If applicable, install reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- ☐ Maintain reasonably up-to-date versions of system security agent software.
- ☐ Educate and train employees and independent contractors on the proper use of the computer security system and the importance of personal information security.

Plan Ahead (continued)

MODEL WRITTEN DATA SECURITY PROGRAM

The following model written data security program was created by the Massachusetts Association of REALTORS® (MAR) and is included in this Toolkit with the Association's permission. This sample policy is provided as a guide to aid in the development of a written data security program tailored to fit your organization's business needs.

COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM ("WISP")

SECTION 1. PURPOSE AND OBJECTIVE:
MAR's objective, in the development and implementation of this WISP, is to create effective administrative, technical and physical safeguards for the protection of Personal Information of residents of the Commonwealth of Massachusetts, and to comply with obligations under 201 CMR 17.00 effective March 1, 2010. This WISP sets forth MAR's procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Personal Information of residents of the Commonwealth.

For purposes of this WISP, "Personal Information" as defined by 201 CMR 17.02 means a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal Information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

The purpose of the WISP is, consistent with MGL Ch. 93H Sec. 2 (a) and 201 CMR 17.01, to (a) Ensure the security and confidentiality of Personal Information; (b) Protect against any anticipated threats or hazards to the security or integrity of such information; (c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

SECTION 2. SCOPE OF WISP:
This WISP specifically seeks to protect Personal Information by:

1. identifying reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information;
2. assessing the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Personal Information;
3. evaluating the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. designing and implementing a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and
5. regularly monitoring the effectiveness of those safeguards:

COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM ("WISP") (continued)

SECTION 3. DATA SECURITY COORDINATOR:
We have designated the Director of Finance and Administration to implement, supervise and maintain MAR's WISP. That designated employee (the "Data Security Coordinator") will be responsible for:

a. Initial implementation of the WISP;

b. Training employees;

c. Regular testing of the WISP's safeguards;

d. Evaluating the ability of each of MAR's third-party service providers, to implement and maintain appropriate security measures for the Personal Information to which we have permitted them access, consistent with 201 CMR 17.00; and requiring such third-party service providers by contract to implement and maintain appropriate security measures.

e. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in MAR's business practices that may implicate the security or integrity of records containing Personal Information.

f. Conducting an annual training session for all employees who have access to Personal Information on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with MAR's requirements for ensuring the protection of Personal Information.

SECTION 4. INTERNAL RISKS:
As part of its regular business actions and in providing services to its members, MAR needs to collect Personal Information as defined by 201 CMR 17.00. MAR recognizes the sensitivity of this information and the need to protect this information, and as such, seeks to limit the amount of Personal Information that is collected. In all cases Personal Information will be collected only in those instances where it is deemed necessary to carry on the business, services and functions of MAR.

MAR recognizes that Personal Information, as defined in 201 CMR 17.00, is regularly collected in the areas identified below. MAR shall take consistent steps to ensure that such information is adequately protected.

1. Employee Records
All records containing Personal Information of employees of MAR shall be maintained by the Director of Finance and Administration. Files shall be restricted and maintained in a locked file cabinet at all times.

2. Educational Courses, Conferences, and Programs
MAR regularly hosts professional education and conferences for members. Payment for such programs is typically made via credit card or debit card. Information received via the MAR website shall be processed on a daily basis and immediately deleted from the MAR website. All electronic records of said Personal Information shall be deleted upon printing. All hard copies of records shall be maintained in locked filing cabinets with limited access for a period of one year. After this period, any hardcopy records shall be destroyed by shredding.

MAR hosts various conferences on an annual basis. As a part of such programs, MAR sells sponsorships to various venders and exhibitors in the Commonwealth. Payment for such services is typically made via credit card. All paper copies of records shall be maintained in locked filing cabinets with limited access for a period determined by the Data Security Coordinator.

Plan Ahead (continued)

COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM ("WISP") (continued)

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures shall be implemented by MAR. To the extent that any of these measures require a phase-in period, such phase-in shall be completed on or before March 1, 2010.

1. A copy of this WISP shall be distributed to each employee who shall, upon receipt of the WISP, acknowledge in writing that he/she has received and read a copy of the WISP.
2. There shall be immediate retraining of employees on the detailed provisions of the WISP. Any new employees hired after March 1, 2010 shall be notified of MAR's WISP, provided with a copy, and shall be trained on the details of this WISP. All such employees shall acknowledge, in writing, receipt of the WISP.
3. The amount of Personal Information collected by MAR shall be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or necessary to comply with other state or federal regulations.
4. Access to records containing Personal Information shall be limited to those persons who are reasonably required to know such information in order to accomplish your legitimate business purpose or to enable us to comply with other state or federal regulations.
5. All security measures shall be reviewed at least annually, or whenever there is a material change in MAR's business practices that may reasonably implicate the security or integrity of records containing Personal Information. The Data Security Coordinator shall be responsible for this review and shall fully apprise MAR Chief Executive Officer of the results of that review and any recommendations for improved security arising out of that review.
6. Terminated employees must return all records containing Personal Information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).
7. A terminated employee's physical and electronic access to Personal Information shall be immediately blocked. Such terminated employee shall be required to surrender all keys to MAR's building. Moreover, such terminated employee's remote electronic access to Personal Information shall be disabled; his/her voicemail access, e-mail access, Internet access, and passwords shall be invalidated. The Data Security Coordinator in conjunction with the Manager of Information Technology shall maintain a highly secured master list of all passwords and keys.
8. Employees must report any suspicious or unauthorized use of customer information to the Data Security Coordinator.
9. Whenever there is an incident that requires notification under M.G.L. c. 93H, §3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of Personal Information for which MAR is responsible.
10. Employees are prohibited from keeping open files containing Personal Information on their desks when they are not at their desks.
11. At the end of the work day, all files and other records containing Personal Information must be secured in a manner that is consistent with the WISP's rules for protecting the security of Personal Information.
12. Access to electronically stored Personal Information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes.
13. Paper or electronic records (including records stored on hard drives or other electronic media) containing Personal Information shall be disposed of only in a manner that complies with M.G.L. c. 93I. MAR shall maintain a paper shredder (or contract for the services of a professional third-party shredding service) on the premises to destroy all paper records containing Personal Information that are no longer needed.
14. Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked.
15. Current employees' user ID's and passwords must be changed periodically. Access to Personal Information shall be restricted to active users and active user accounts only.

SECTION 5. EXTERNAL RISKS:
To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures shall be completed on or before March 1, 2010:

1. MAR shall, at all times, maintain an up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Personal Information, installed on all systems processing Personal Information.
2. MAR shall, at all times, maintain an up-to-date version of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing Personal Information.
3. Certain MAR staff maintain portable electronic smart phones and laptops owned by MAR and provided to staff for official employment duties. To the extent technically feasible, all Personal Information stored on laptops or other portable devices shall be encrypted, as well as all records and files transmitted across public networks or wirelessly, to the extent technically feasible.
4. All computer systems must be monitored for unauthorized use of or access to Personal Information.
5. There shall be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a location.

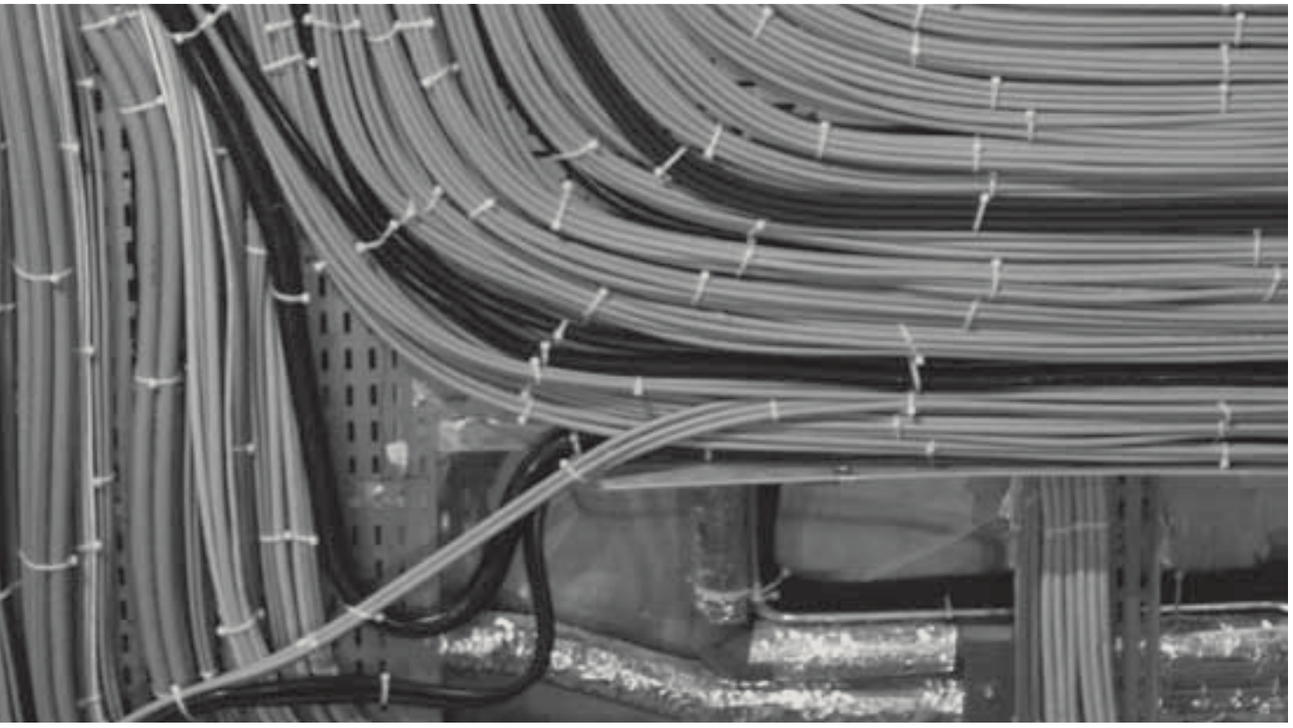
Plan Ahead (continued)

DATA SECURITY BREACH NOTIFICATION

As previously mentioned, almost every jurisdiction in the United States has a law making it mandatory for a business to provide notice to interested parties when that business has experienced a security breach. In many cases, these laws include requirements regarding the means, content, and timing of the notification. They also specify what constitutes a security breach and what actions a business may be required to take following a breach. Although the laws vary, many are similar in that they require the following elements to be included in the content of a breach notification:

- Description of what happened (unless limited by applicable law)
- Type of protected data involved
- Actions to protect data from further unauthorized access
- What the company will do to assist affected persons
- What affected persons can do to assist themselves
- Contact information for company inquiry response system
- Contact information for local and federal government authorities

When a security breach occurs, there is a lot to do and there may not be much time to craft a notification letter from scratch. That is why it is a good idea to develop a model notice template that can be tailored easily to include the particulars of the incident. Please remember that the content of your notice will be governed by the laws of the various states in which the affected parties reside and each of those laws should be consulted when drafting your own model template.



CHECKLIST FOR DRAFTING A BREACH NOTIFICATION POLICY

The following checklist presents issues you should consider—and perhaps address—in your business's breach notification policy and potential solutions to those issues.

☐ **Individual or individuals responsible for responding to a security breach**
- ○ Information Technology Systems employee
- ○ Human Resources employee
- ○ Legal Counsel
- ○ Public Communications/Media Relations employee
- ○ A security breach response team that includes representatives from more than one department

☐ **Action upon learning or being notified of a security breach**
- ○ Immediately investigate the incident
- ○ Isolate all affected systems to limit further data loss
- ○ Contact the individual or team responsible for responding to the breach
- ○ Determine whether law enforcement should be notified

☐ **Information to be collected related to the breach**
- ○ Date, time, duration, and location of breach
- ○ How the breach was discovered, who discovered the breach, and any known details surrounding the breach, for example:
  - Method of intrusion
  - Entry or exit points
  - Paths taken
  - Compromised systems
  - Whether data was deleted, modified and/or viewed
  - Whether any physical assets are missing
- ○ Details about the compromised data:
  - A list of affected individuals and type
  - Data fields
  - Number of records affected
  - Whether any data was encrypted (if so, which fields)
  - What personal information has been compromised
- ○ Determine whether special consultants are necessary to capture relevant information and perform forensics analysis

☐ **Implications of the breach**
- ○ Consider whether other systems are under a threat of immediate or future danger
- ○ Determine whether you are legally obligated to provide notification about the breach and to whom
  - Residents of your state
  - Residents of other states
  - State agencies
  - Law enforcement
  - Credit reporting agencies
- ○ Determine whether you are contractually obligated to provide notification about the breach
- ○ Consult legal counsel regarding liability, litigation risk, law enforcement investigations, and other legal concerns

☐ **Procedures to be followed in the event that written notification is required or elected**
- ○ Prepare a list of persons to be notified
- ○ Choose a mode of communication for notification, if not already mandated by law
- ○ Draft a notice that complies with applicable laws and contractual obligations
- ○ Consider whether to offer certain remediation services to assist affected persons
- ○ Be sure to comply with any legal or contractual timing requirements

☐ **Action following a breach and notification**
- ○ Prepare an online FAQ and document inquiries and responses
- ○ Review information technology systems and physical security
- ○ Assess operational controls and consider revising company policies or procedures regarding data collection, retention, or storage
- ○ Assess the need for additional employee training in data protection policies and processes
- ○ Review agreements and policies to determine whether any updates or modifications need to be made, including agreements with third parties that handle personal information, website privacy notices and terms of service, agreements with customers or other third parties, and employee handbooks and policies
- ○ Evaluate your response to the breach

Plan Ahead (continued)

MODEL BREACH NOTIFICATION TEMPLATE

The following model breach notification template was created by the State of California Office of Information Security & Privacy Protection.[14] This model is intended to provide guidance for developing a model notice template tailored to your business's specific circumstances.

[14] State of California Office of Information Security & Privacy Protection, Sample Breach Notice: Social Security Number Only, available at: http://www.cio.ca.gov/OIS/Government/library/samples.asp.

[Salutation]

We are writing to you because of a recent security incident at *[name of organization]*.

[Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files by following the recommended privacy protection steps outlined in the enclosure. For more information on identity theft, you may visit the website of the California Office of Information Security & Privacy Protection at **www.privacy.ca.gov**.

We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information about this incident, please contact *[name of the designated agency official or agency unit handling inquiries]* at *[toll-free phone number]*.

[Closing]

Enclosure *[Enclose information regarding what steps to take following a security breach. A sample enclosure is available at:* **http://www.privacy.ca.gov/res/docs/pdf/Security_Breach_First_Steps.pdf**.*]*

Privacy Policies

As stated in the Introduction, a privacy policy is a document that discloses the ways your business collects, shares, protects, and destroys personal information. Often, the privacy policy is made available on a business's website, although that practice is only required for certain types of businesses. Currently, federal privacy laws pertain only to the following types of businesses that: knowingly collect information about children under the age of 13; collect, use, or share an individual's financial information; or provide or use information related to healthcare services. However, some states, such as California[15], require commercial websites that collect personal information regarding its residents to conspicuously post a privacy policy on the website.

Even though no comprehensive federal regulation currently exists that specifically applies to real estate associations or brokerages, several relevant bills have been introduced by Congress and may be adopted in the near future. These bills pertain not only to the online collection of information, but offline collection as well. And, if your business collects information from a resident of a state with laws requiring privacy policies, then it is a good idea to have a Privacy Policy in place and to provide a link to that Privacy Policy on each page of your website. This section of the Toolkit will provide a checklist of issues to consider and potentially address when drafting a privacy policy that fits your business needs and some possible solutions to those issues. A copy of NAR's Privacy Policy is also included for guidance.

[15] See California Online Privacy Protection Act of 2003 — Business and Professions Code sections 22575-22579.

CHECKLIST FOR DRAFTING A WEBSITE PRIVACY POLICY

The following checklist presents issues you should consider — and perhaps address — in your business's privacy policy and potential solutions to those issues.

☐ **How notice is provided to consumers**
- ○ Clear and conspicuous
- ○ Accessible through a direct link from each page of the website
- ○ May be amended with (or without) notice

☐ **Type of information that is collected about a user**
- ○ Information volunteered by the user
- ○ Domain name or IP address
- ○ Type of browser or operating system being used
- ○ Date and time of visit
- ○ Statistical information about which Web pages a user visits
- ○ Websites the user visited prior to coming to your website
- ○ Websites the user visits after leaving your website
- ○ Minors are prohibited from volunteering any personal information

☐ **How the information is collected**
- ○ Volunteered by the user
- ○ Cookies or other automatic collection of information

☐ **Why the information is being collected**
- ○ To improve the content of your website
- ○ To help you understand how people are using your services
- ○ Send notices to the user of updates to the website or new products
- ○ Shared with affiliates, other third parties

☐ **What happens to the information collected**
- ○ Explain how the information is stored
- ○ Data retention/disposal policy

☐ **User's ability to obtain access to the collected information**
- ○ Describe under what circumstances the user may access his information
- ○ The user may contact you with inquiries or complaints regarding the handling of collected information
- ○ The user may opt-out of collection of the information

☐ **Identity and contact information of the website operator**

☐ **Effective date of the privacy policy**

Model Privacy Policies

The following privacy policies were created by the NATIONAL ASSOCIATION OF REALTORS® and are maintained on *REALTOR.org* and Realtoractioncenter.com, respectively. These policies are intended to provide an example for developing a privacy policy tailored to your business's specific circumstances.

REALTOR.ORG PRIVACY POLICY

Effective Date: 03/04/2009

We recognize the importance of protecting the personal information you provide at websites owned and/or controlled by the NATIONAL ASSOCIATION OF REALTORS® (NAR). One of the National Association's sites, REALTOR.com®, has posted its own "privacy polices" and "terms of use." For the rest of the National Association's websites, we maintain the following privacy policy:

1. We gather the following types of information needed to process your transactions, fulfill your requests, and maintain our membership records:
   - Contact information you provide (for example, your personal and business addresses, phone and fax numbers, firm affiliations and titles).
   - Tracking information that our Web server automatically recognizes each time you visit one of our sites or communicate with us by e-mail (for example, your domain name, your e-mail address, and what pages you visit).
   - Information you volunteer, via applications or surveys (for example, education, designations, specialties, affiliations with other real estate organizations and general demographic data).
2. We use this information to:
   - Improve and customize the content and layout of our sites and other communications tools, such as *REALTOR*® Magazine online and print.
   - Notify you of updates to our sites.
   - Notify you of relevant products and services.
   - Notify you of upcoming events and programs.
   - Compile specialty directories about which you will be made aware.
   - Track usage of our sites.
   - Assist local and state REALTOR® associations and affiliated Institutes, Societies and Councils in membership tracking and for their use for purposes similar to those listed above.
3. E-mail contact information. NAR does not share, sell or trade e-mail addresses. NAR may use your e-mail address to directly send you information and may provide you with online informational or marketing messages that have been approved by NAR together with other communications to which you have subscribed.
4. Other forms of contact information. Forms of contact information other than e-mail address (e.g., street address) may be listed in the membership directories available on *REALTOR.org* and REALTOR.com®. NAR will not share, sell or otherwise provide this contact information about you except for the following purposes:
   - Partners in our REALTOR Benefits® Program for the limited purpose of notifying you of NAR-approved promotions.
   - Exhibitors at REALTOR® trade shows for the limited purpose of contacting you one time immediately before and after trade shows, through marketing vehicles approved by NAR.
   - Other vendors for the limited purpose of contacting targeted groups of members, through marketing vehicles approved by NAR.
   - When required by law or valid legal process, or to protect the personal safety of our members or the public.
   - Some or all of the data collected during promotions or contests on our sites that are sponsored by third parties may be shared with the sponsor for the limited purpose of a one-time marketing follow-up by the sponsor. If information about you will be shared with a sponsor, you will be notified prior to your participation in the promotion or contest and you can decide not to participate in the promotion or contest.
5. Credit information that you and credit authorizers provide when you make payments by credit card or electronic check for products, dues or other services via the REALTOR® Electronic Commerce Network ("E-Commerce Network") will only be used to process the transactions you request. This information will be provided to and maintained by reputable credit reporting databases, but will never be sold, shared or provided to other third parties.
6. We maintain security procedures and standards, which we believe are as safe as today's technology permits. We test these procedures and modify them regularly as new technologies become feasible.
7. We utilize a strict Opt-Out policy for sending online notifications regarding services, products and programs. You may adjust your Communication Preferences by reviewing your *REALTOR.org* registration. Just log in first. Then you can change your preferences. (Examine and update your existing account).
8. You may edit your personal contact information directly in the NRDS system or by contacting your local REALTOR® association.
9. Some of our sites contain advertising placed by advertising networks pursuant to agreements between the National Association and the advertising network. We do not control these advertising networks, the sites of third parties reached through links on our site or their information collection practices, and the National Association will not be responsible for the activities of these third parties. The advertising network uses cookies to collect certain non-personally identifiable information when you click on the banner ads appearing on our sites. This information is collected by the advertising network for purposes of measuring and reporting on the advertising to advertisers and the National Association. The advertising network may also aggregate the information for certain other statistical and reporting purposes.

500 New Jersey Avenue, NW • Washington, DC 20001-2020
800.874.6500 • www.REALTOR.org

NATIONAL ASSOCIATION *of* REALTORS®