Important Topics in Real Estate

April 15, 2010

THE LAW OFFICE of
DAVID R. ROCHEFORD, JR., P.C.

www.TheBestClosings.com

Find us on Facebook LinkedIn twitter

THE LAW OFFICE of
DAVID R. ROCHEFORD, JR., P.C.

Contents:

"Our mission is to provide the finest quality service and expertise in the title and settlement service business. This means timely and accurate transactions that exceed all expectations. We treat every customer as a valued partner and every transaction as a unique project, worthy of personalized attention and innovative solutions. Our staff is empowered and accountable to make customer satisfaction their number-one priority, while doing business with uncompromised integrity."

- The Law Office of David R. Rocheford, Jr., P.C.

THE LAW OFFICE of DAVID R. ROCHEFORD, JR., P.C.

Summary of Recent RESPA and Regulation "Z" Reform

Key Features of RESPA Reform

- New style 3 page Good Faith Estimate (GFE):
- Must be provided to borrower within 3 days of receipt of a complete application.
- Must match HUD-1 at closing within certain tolerances.
- Except for "changed circumstances" GFE cannot change prior to closing.
- Changed circumstances - is defined as: (1) Acts of God, war, disaster, or other emergency; (2) Inaccurate information being relied upon, (3) New information particular to the borrower or transaction that was not relied upon; or (4) Other circumstances that are particular to the borrower or transaction, including boundary disputes, the need for flood insurance, or environmental problems.

New style 3 page HUD-1 Settlement form:

- HUD-1 Settlement Statement must match GFE within certain tolerances.
- Lender must correct any intolerance within 30 days of closing.

With limited exception fees quoted to a borrower on GFE cannot change prior to closing:

- Lender Fees and Points cannot change.
- Some settlement fees can change up top 10%.
- Fees for borrower chosen services may change.
- Escrows for taxes and insurance and per diem interest may change.

Truth in Lending or Regulation "Z" Changes

- The lender may not collect any fees before the disclosure is provided, except for a reasonable fee for obtaining a credit report.

- The closing may not take place until expiration of a 7 day waiting period after the consumer receives the early disclosure.

- If the annual percentage rate (APR) changes by more than 0.125 (1/8th) of a percent, the lender must provide a corrected disclosure to the borrower and wait an additional 3 business days before closing the loan.

- A copy of the property appraisal must be delivered to the mortgage applicant at least three days prior to closing.

Reference:

Presentation material: www.thebestclosings.com/2010HUD

www.TheBestClosings.com

THE LAW OFFICE of
DAVID R. ROCHEFORD, JR., P.C.

New lead paint regulations go into effect in Mass. on April 22, 2010.

Although the new regulations do not immediately or directly impact Realtors® and real estate agents, contractors will now be required to be certified by the Environmental Protection Agency in order to perform even the simplest repairs or renovations to properties built before 1978. According to the state Childhood Lead Poisoning Prevention Program as much as 30 percent of childhood lead poisoning cases in Massachusetts involve exposure to lead dust caused by renovation work. That is a serious figure considering the devastating, life long effects of lead poisoning. Homeowners who have work performed on their property by contractors, including painters, plumber, electricians and carpenters, must ensure that the contractor is "EPA Lead Safe Certified."

The rule can be summarized in four parts:

1. **Training and Certification**
   Beginning in April 2010, firms working in pre-1978 homes will need to be certified. In addition to firm certification, an employee will also need to be a Certified Renovator. This employee is responsible for training other employees and overseeing work practices and cleaning. The training curriculum for certification, in development with the EPA, will be an eight-hour class with two hours of hands-on training. Both the firm and renovator certifications are valid for five years.

2. **Work Practices**
   Once work starts on a pre-1978 renovation, the Certified Renovator has a number of responsibilities. Beginning with distributing EPA's Renovate Right brochure to the homeowner and having them sign the pre-renovation form in the booklet. Before the work starts the Certified Renovator will post warning signs outside the work area and supervise setting up containment to prevent spreading dust.

   The rule lists specific containment procedures for both interior and exterior projects. It forbids certain work practices including open flame or torch burning, use of a heat gun that exceeds 1100 degrees F, and high-speed sanding and grinding unless the tool is equipped with a HEPA exhaust control. Once the work is completed, the regulation specifies cleaning and waste disposal procedures. Clean up procedures must be supervised by a Certified Renovator.

3. **Verification and Record Keeping**
   After clean up is complete the Certified Renovator must verify by matching a cleaning cloth with an EPA verification card. If the cloth appears dirtier or darker than the card, the cleaning must be repeated. A complete file of records on the project must be kept by the certified renovator for three years. These records include, but aren't limited to verification of owner-occupant receipt of the Renovate Right pamphlet or attempt to inform, documentation of work practices, Certified Renovator certification, and proof of worker training.

4. **Exemptions**

   - The home or child occupied facility was built after 1978.
   - The repairs are minor, with interior work disturbing less than six sq. ft. or exteriors disturbing less than 20 sq. ft.
   - The homeowner may also opt out by signing a waiver if there are no children under age six frequently visiting the property, no one in the home is pregnant, or the property is not a child-occupied facility.
   - If the house or components test lead free by a Certified Risk Assessor, Lead Inspector, or Certified Renovator.

In pending real estate transactions real estate professionals should be certain that homeowners are aware of the new regulations, particularly if a seller is doing renovations or repairs to the property in preparation for the sale. Without doubt there will be a new form or two to be executed at the time of listing and or at closing.

Buyers purchasing properties constructed prior to 1978 (and there mortgage lenders) will certainly be looking for representation from sellers that the property is in compliance with the new regulation. Expect to see new language included in purchase and sale agreements accordingly.

www.TheBestClosings.com

THE LAW OFFICE of
DAVID R. ROCHEFORD, JR., P.C.

New Oil Heating System Law Affects Homeowners

On July 1 2010 a new Massachusetts law goes into effect that will concern certain homeowners. The new law requires that all 1 to 4 family residential dwellings serviced by a home heating oil system meet new safety standards.

Homeowners using home heating oil must have either an oil supply safety valve or an oil supply line with a special protective sleeve.

Homes build after January 1990 should already be in compliance with the new law and would likely have one or both of these safety features installed.

However, homes constructed prior to then may not have such safety features and are required to be in compliance and upgraded by July 1, 2010.

There are limited exemptions and an upgrade is estimated to cost between $150.00 and $350.00.

If you represent a home seller with a property constructed before 1990 confirm with them that they are aware of the new law and that they understand that they will need to be in compliance in order not to complicate a potential sale.

If you represent home buyers buying a home subject to the law inform them of the new law and ensure that the seller is incompliance before closing.

Reference:

Digest of the new law: http://www.mass.gov/dep/cleanup/laws/hhsl.htm

PDF fact sheet for buyers and sellers: http://www.mass.gov/dep/cleanup/laws/hhsl.pdf

www.TheBestClosings.com

Homeowner Oil Heating System Upgrade and Insurance Law

By July 1, 2010, you must upgrade your home heating system equipment to prevent leaks from tanks and pipes that connect to your furnace.

This fact sheet contains important information for those who heat their homes with oil. By July 1, 2010, you must upgrade your home heating system equipment to prevent leaks from tanks and pipes that connect to your furnace. By making a relatively small expenditure now, you can prevent a much greater expense in the future.

Massachusetts has a new law to address oil leaks from home heating systems (see Chapter 453 of the Acts of 2008). This law has two major provisions that require:

- the installation of either an oil safety valve or an oil supply line with protective sleeve on systems that do not currently have these devices; and
- insurance companies that write homeowner policies to offer coverage for leaks from heating systems that use oil.

Most homeowner policies do not currently include such coverage, leaving many to pay for costly cleanups out of their own pocket. Although it is mandatory that insurance companies offer this coverage, the insurance is an optional purchase for homeowners. The effective date for both provisions is July 1, 2010.

Who must take action?

Owners of 1- to 4-unit residences that are heated with oil must already have or install an oil safety valve or an oil supply line with a protective sleeve, as shown in the diagram. Installation of these devices must be performed by a licensed oil burner technician. Technicians are employed by companies that deliver home heating oil or are self-employed. It is important to note that heating oil systems installed on or after January 1, 1990 most likely are already in compliance because state fire codes implemented these requirements on new installations at that time.

Who is exempt?

Homeowners are exempt from taking these leak prevention steps if:

- the oil burner is located above the oil storage tank and the entire oil supply line is connected to and above the top of the tank OR
- an oil safety valve or oil supply line with protective sleeve was installed on or after January 1, 1990, AND
- those changes comply with the oil burning equipment regulations; a copy of the oil burner permit from the local fire department may be used to demonstrate compliance.

Why comply?

Not only is complying with the new law required, it makes good financial and environmental sense. Homeowners who take these preventive measures can avoid the disruption and expense that can be caused by heating oil leaks. A leak may result in exposure to petroleum vapors in your home. If the leak reaches the soil or groundwater beneath your house, then a cleanup must be performed to restore your property to state environmental standards. Leaks that affect another property or impact drinking water supply wells can complicate the cleanup and increase the expense. Each year, several hundred Massachusetts families experience some kind of leak.

What will an upgrade cost?

The typical cost of installing either an oil safety valve or oil supply line with a protective sleeve ranges from $150 - $350 (including labor, parts, and local permit fees).

For those households that meet certain income criteria, financial assistance of up to $300 is available through the Low Income Home Energy Assistance Program (LIHEAP). For more information on financial assistance, see the Department of Housing and Community Development Web site at http://mass.gov/dhcd or call them at 1-800-632-8175.

What could it cost to cleanup a leak?

The cleanup cost for a “simple” leak can be as much as $15,000. In cases where the leak affects the groundwater or is more extensive, the cleanup costs can reach $250,000 or more.

What kind of insurance is available?

To be eligible for the new insurance coverage, homeowners must ensure that their oil heating systems are in compliance with the new law. Homeowners who have been certified to be in compliance with (or exempt

from) the leak prevention measures qualify to purchase insurance that:

- ▷ provides "first party coverage" of at least $50,000 for the cost of cleaning up a leak to soil, indoor air, or other environmental media from a home heating system at the residence itself and reimbursement for personal property damage, AND
- ▷ provides "third party coverage" of at least $200,000 for the cost of dealing with conditions on and off the insured's property because the leak from this system has or is likely to affect groundwater or someone else's property. The coverage also includes costs incurred for legal defense, subject to a deductible not to exceed $1,000 per claim.

What should I do next?

① Determine whether you have had an oil safety valve or new oil supply line with protective sleeve installed since January 1, 1990. If you have, your permit from the fire department for the installation can be used to document your compliance. You can request a copy from the fire department if the permit is on file, or a licensed oil burner technician can certify that status on a form.

② If you do not have an oil safety valve or oil supply line with protective sleeve in place, have one or the other installed and certified. Either contact your oil delivery company to ask if they employ a licensed oil burner technician or find a service person in your area. (A list of licensed technicians can be viewed at http://db.state.ma.us/dps/licenseelist.asp. Click on the "individuals" tab, scroll down to and then select "Oil Burner – Technical Certificate" in the "select a license type" box, type in your city or zip code, and click "select").

③ Consider buying insurance coverage for the cleanup of a leak.

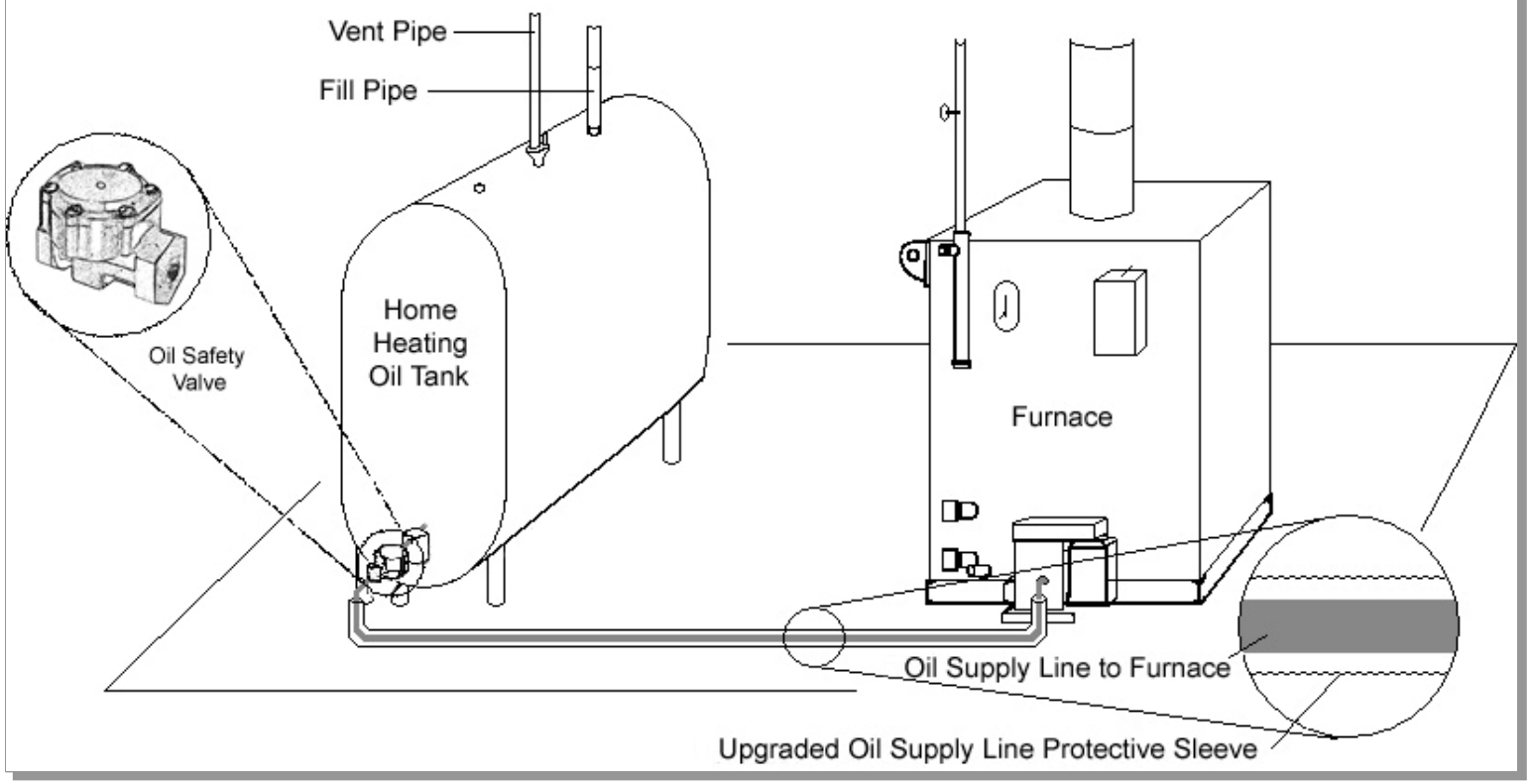
- ▷ Determine whether your existing policy provides oil leak coverage.
- ▷ If it does not, consider calling your homeowner insurance agent to amend the policy to include this coverage.

MASS. DEPARTMENT OF FIRE SERVICES
Commonwealth of Massachusetts

Massachusetts Department of ENVIRONMENTAL PROTECTION

Find more information at http://mass.gov/dep/cleanup/laws/hhsl.htm

Diagram: Above-Ground Home Heating Oil System Leak Prevention Upgrades



THE LAW OFFICE of DAVID R. ROCHEFORD, JR., P.C.

New Foreclosure Alternative Program May Offer Relief to Homeowners

The Home Affordable Foreclosure Alternatives (HAFA) program is a part of the Home Affordable Modification Program (HAMP), and offers a streamlined process for short sales and deeds-in-lieu of foreclosure. HAFA will allow homeowners to discharge their first mortgage debt without the credit-destroying step of foreclosure. The program also offers a $1,000 incentive to banks to permit short sales and a $1,500 bonus to homeowners for the purpose of relocation.

The HAFA program has eligibility guidelines:

- The property must be the owner's principal residence
- The first mortgage must have originated before 2009
- The unpaid principal must be less than $729,750 for a single-family dwelling
- The borrower's monthly payment must exceed 31% of their gross income
- The mortgage must either be delinquent or a default be reasonably foreseeable.

If borrowers meet the program requirements they will receive pre-approved short sale terms from their lender, which will include a minimum acceptable proceeds figure for the sale. The homeowner will be required to list the property for sale with a Realtor® and close within 120 day, extensions may be permitted up to a total of 12 months.

Based on the short sale agreement with the lender, HAFA requires property owners to be fully released from any future liability on their first mortgage debt, and in some cases, subordinate debts, so that when the home is sold, the borrower is free and clear of their mortgage.

The program ends on December 31, 2012. HAFA does not apply to FHA or VA loans. There is an extensive amount of paperwork to be completed to participate in the program, Homeowners wishing to take advantage of the relief offered are encouraged to work with a experienced Realtor®.

www.TheBestClosings.com

THE LAW OFFICE of DAVID R. ROCHEFORD, JR., P.C.

Mass. Smoke/Carbon Monoxide Detector Law Effective April 5, 2010

2 Types of Smoke Detector Technology

The two most common methods of fire/smoke detection technology currently used is either ***ionization*** or ***photoelectric*** based.

Ionization sensors feature a constant current flowing between two electrodes. When smoke strikes the device, it impedes the current between the electrodes and causes the alarm to set off.

Ionization sensors are usually quicker to go off than photoelectric detectors. The problem with ionization detectors is that they are not able to distinguish between smoke and steam.

This makes them prone to false alarms when steam from a shower or other source interrupts the current. This is particularly true when the ionization detector is located near a kitchen or bathroom.

Photoelectric sensors send a beam of light between two sensors. This beam passes in front of the sensors in a direct line. When smoke cuts across the path of the light beam, some light is dispersed by the smoke particles causing it to activate the alarm. Photoelectric detectors are less sensitive to false alarms from steam or cooking exhaust fumes but may take longer than ionization detectors to operate.

Another major concern is that ionization detectors do not offer the best protection in fires that smolder. Fires that smolder are some of the deadliest fires nationally. Photoelectric smoke alarms are more sensitive to smoldering, smoke producing fires. Most of the residential dwellings in the country have ionization detectors which are more sensitive to flames.

Tests of both types of alarms show that in smoke producing fires photoelectric detectors sound first and it takes nearly 17 minutes longer before an ionization alarm sounds.

New Fire Detector Regulations

Since there are strengths and weaknesses between photoelectric and ionization smoke detectors, the Board of Fire Prevention Regulation has passed a new regulation (527 CMR 32.00).

According to the new regulation, owners of certain residential buildings will be required to install and maintain both the ionization and photoelectric smoke detectors.

While the new regulation does not change the locations where smoke detectors are required, it does call for the installation of both technologies in certain locations.

Under the new regulation, an ionization detector can not be placed within 20 feet of a kitchen or a bathroom containing a shower or a tub. In these locations only a photoelectric detector is allowed.

In order to comply with the law you can either install two separate detectors that have both technologies or by installing one that utilizes both.

What Properties Are Affected By The New Regulation?

In order to determine if a property is affected by this change you may consider checking with the local fire department. According to the new amendment the following types of properties are impacted by the new regulation:

- Residential buildings under 70 feet tall and containing less than six dwelling units.
- Residential buildings not substantially altered since January 1, 1975, and containing less than 6 residential units.
- All residential buildings sold or transferred after April 5, 2010, which are less then 70 feet tall, have less than six units, or have not been substantially altered since January 1, 1975.

For all properties in these categories, compliance is mandated by April 5, 2010. It should be noted that the law does not apply to these larger buildings or those which were substantially altered since January, 1975, as these properties already were required to upgrade their fire safety systems under other existing laws.

One other important note regarding smoke detectors: Many towns require hard wired smoke detectors and NOT battery operated. You should make certain you know what the requirement is for the town where the property is located in. As a general rule according to the State fire Marshall's office, the law is as follows:

- Homes built after 1975 are required upon sale or transfer to comply with the State Building Code in effect at the time of construction.
- Homes built before 1975 are required upon sale or transfer to comply with the requirements of MGL c. 148, §26E(A); and
- Homes built between 1975 and 1998 are required to have hard wired interconnected smoke detectors outside the bedrooms and one detector on each floor at the top of the stairs. The smoke detector at the top of the stairs can be the same detector that is required outside the bedroom.

- Homes built after 1998, smoke detectors are required to be interconnected and have a battery backup. Smoke detectors are required in each bedroom, outside the bedroom and at the top of each flight of stairs. A single detector can satisfy multiple location requirements, if sited properly. There must also be one smoke detector on each level and one smoke detector for each 1,200 square feet of living space.

  The requirements for newer construction also apply to additions and/or renovations where a bedroom is either added or substantially altered. If an addition or renovation involves adding or substantially changing a bedroom, the entire house, including existing bedrooms must be brought up to the present standard according to the Massachusetts State Building Code (780 CMR), regardless of when the original home was built.

Carbon Monoxide detectors are required in any residence that has fossil-fuel burning equipment including, but not limited to, a furnace, boiler, water heater, fireplace or any other apparatus, appliance or device; or has enclosed parking within its structure.

According to the carbon monoxide regulations, you need to have a detector on each finished level of the home. Further there must be a detector placed within ten feet of all the bedroom doors. The detectors do not need to be hard wired. A plug-in or battery operated detector meets the requirements and usually the most viable choice. Here are all the types are carbon monoxide detectors that are allowed:

- Battery powered with battery monitoring
- Plug-in (AC powered) units with battery backup
- Hardwired AC primary power with battery backup
- Low-voltage or wireless alarms with secondary power; and
- Certain combination smoke detectors and CO alarms

www.TheBestClosings.com

THE LAW OFFICE of DAVID R. ROCHEFORD, JR., P.C.

Massachusetts Privacy Law - 201 CMR 17 Compliance

Massachusetts privacy law requires businesses to implement security controls to protect systems containing Massachusetts resident's personal information from data loss.

What is Mass 201 CMR 17?

In an effort to protect Massachusetts residents from the rising incidence of fraud and identity theft from data loss, the State of Massachusetts has implemented aggressive regulatory requirements to protect personal information. The state now requires mandatory compliance with 201 CMR 17.00 - Standards for the Protection of Personal Information of Residents of the Commonwealth (also known as just 201 CMR 17, or the Massachusetts Privacy Law). Building on California's landmark security regulation SB-1386, Massachusetts Privacy Law establishes a minimum standard to be met for the protection of Massachusetts resident's personal information (PI) contained in both paper and electronic records. For the purpose of being compliant with the new Massachusetts data privacy law, PI 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 the resident:

- Social Security number;
- Driver's license number or Massachusetts identification card number;
- 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; or
- A biometric indicator.

The Massachusetts data privacy law has set a new level in state security laws by regulating both private and public sector entities that handle Massachusetts resident's sensitive data, regardless of where that entity is located. The law is intended to bring entities into alignment with both federal and industry security laws, including the Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA) enforced by the Federal Trade Commission (FTC) and Payment Card Industry Data Security Standards (PCI-DSS) security standards overseen by the PCI Security Standards Council. Its process and technical controls are aimed at preventing criminal activity from causing data breaches of either paper or electronic records containing PI. The requirement of securing electronic records includes PI on databases, laptops, applications, portable devices, and just about any other system in which electronic PI data can be either in transit or at rest.

Who needs Mass 201 CMR 17?

All persons, corporations, associations, partnerships or other legal entities with systems containing Massachusetts resident's personal information in transit or at rest are responsible for complying with the 201 CMR 17 regulations by March 1, 2010. However, the regulations also require businesses to complete internal and external security risk assessments prior to the effective date. The regulation applies regardless of whether the entities or the data is either inside or outside state borders, and applies equally to private and public sector organizations.

Penalties for non-compliance

The penalties for non-compliance with 201 CMR 17 are enforced through Massachusetts General Law Title XV: Regulation of Trade, chapter 93A, section 4. Violators may be faced with a civil penalty of $5,000 for each violation, are required to pay the reasonable costs of investigation and litigation of such violation (including reasonable attorney's fees), and are subject to additional civil action since 201 CMR 17 creates a baseline standard that allows plaintiffs in civil suits to argue that a business that lost data was negligent. Title XV also requires any data breach be reported to both the Office of Consumer Affairs and Business Regulation (OCABR) and the Attorney General.

What you need to be Mass 201 CMR 17 compliant

The new Massachusetts Privacy Law requires the following criteria be met:

- An internal and external risk assessment of the human, physical, technical environment based on the criteria outlined in 201 CMR 17
- the computer security provisions in the regulation use a risk-based approach that comply to the extent that it is technically feasible, meaning that reasonable means must be used to accomplish a required result if there is a reasonable technology is available
- the results of the internal and external risk assessments must be documented in a Written Comprehensive Information Security Program (WISP)
- the scope of the WISP must be reviewed at least on an annual basis or whenever there is a change in business practices that may impact security controls

The OCABR published the 201 CMR 17 Compliance Checklist as an aid to be used by either organizations themselves or their auditors when conducting their risk assessment. However, additional guidance on how and where to submit risk assessment results is expected from the state prior to the March 2010 deadline.

Reference: http://www.mass.gov/Eoca/docs/idtheft/compliance_checklist.pdf

www.TheBestClosings.com

COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION
10 Park Plaza – Suite 5170, Boston MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

GREGORY BIALECKI
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

BARBARA ANTHONY
UNDERSECRETARY

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)

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

- Does the WISP provide for immediately blocking terminated employees' physical and electronic access to PI records (including deactivating their passwords and user names)?
- Have you taken reasonable steps to select and retain a third-party service provider that is capable of maintaining appropriate security measures consistent with 201 CMR 17.00?
- Have you required such third-party service provider by contract to implement and maintain such appropriate security measures?
- Is the amount of PI that you have collected limited to the amount reasonably necessary to accomplish your legitimate business purposes, or to comply with state or federal regulations?
- 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?
- 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?
- In your WISP, have you specified the manner in which physical access to PI records is to be restricted?
- Have you stored your records and data containing PI in locked facilities, storage areas or containers?
- 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?
- 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?
- 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

- Do you have in place secure authentication protocols that provide for:
  - □ Control of user IDs and other identifiers?
  - □ A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)?
  - □ 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?
  - □ Restricting access to PI to active users and active user accounts?
  - □ Blocking access after multiple unsuccessful attempts to gain access?
- Do you have secure access control measures that restrict access, on a need-to-know basis, to PI records and files?

- 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?
- 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?
- Do you, to the extent technically feasible, encrypt all PI stored on laptops or other portable devices?
- Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?
- 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?
- 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?
- Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?