Massachusetts Department of Revenue *Division of Local Services*
Navjeet K. Bal, Commissioner Robert G. Nunes, Deputy Commissioner & Director of Municipal Affairs

E-billing
Property Tax and Municipal Utility Bills

Prepared for Massachusetts Collectors & Treasurers Association – April 2011

G.L. c 60 § 3A - FORM OF TAX BILL OR NOTICE AS AMENDED BY ST. 2010, c. 188, § 54

Section 3A. **(a)** Each bill or notice shall be in a form approved by the commissioner and shall summarize the deadlines under section 59 of chapter 59 for applying for abatements and exemptions. Each bill or notice shall also have printed on it the last date for the assessed owner to apply for abatement and for exemptions under clauses other than those specifically listed in said section 59 of said chapter 59. Except in the case of a bill or notice for reassessed taxes under section 77 of said chapter 59, each bill shall also have printed on it the last date on which payment can be made without interest being due. If a bill or notice contains an erroneous payment or abatement application date that is later than the date established under said chapter 59, the date printed on the bill or notice shall be the deadline for payment or for applying for abatement or exemption, but if the error in the date is the wrong year, the due date shall be the day and month as printed on the bill but for the current year. The commissioner may require, with respect to a city or town, that the tax bill or notice include such information as the commissioner may determine to be necessary to notify taxpayers of changes in the assessed valuation of the property. Each bill or notice for real or personal property tax shall have printed thereon in a conspicuous place the tax rate for each class within the town, as determined by the assessors. In addition, each bill or notice for a tax upon real property shall identify each parcel separately assessed by street and number or, if no street number has been assigned, by lot number, name of property or otherwise, shall describe the land, buildings and other things erected on or affixed to the property and shall state for each such parcel the assessed full and fair cash valuation, the classification, the residential or commercial exemption, if applicable, the total taxable valuation and the tax due and payable on such property. **If the assessors have granted the owner an exemption under any clause specifically listed in said section 59 of said chapter 59, the bill or notice of such owner may also show the exemption and the tax, as exempted, that is due and payable on such property.**

(b) The collector may issue the bill or notice required by section 3 in electronic form, provided that the electronic bill or notice meets the standards set forth in subsection (a). An electronic bill or notice issued shall be under voluntary programs established by the collector, with the approval of the board of selectmen or mayor, as the case may be. No political subdivision shall require a taxpayer to take part in an electronic billing system or program.

(c) The collector may include in the envelope or electronic message in which a property tax bill is sent those bills or notices for rates, fees and charges assessed by the city or town for water or sewer use, solid waste disposal or collection or electric, gas or other utility services as may be authorized by ordinance or by-law; provided, however, that the bills or notices shall be separate and distinct from the property tax bills. The ordinance or by-law may authorize the collector, upon vote of any municipal water and sewer commission established by the city or town under chapter 40N or by special act, to include bills or notices for rates, fees or charges assessed by the commission for water or sewer use.

(d) The collector may, with the approval of the board of selectmen or mayor, as the case may be, include in the envelope **or electronic message** in which a property tax bill is sent nonpolitical municipal informational material; provided, however, that if such nonpolitical municipal informational material is mailed, it shall not be included if the material causes an increase in the postage required to mail the tax bill.

SECTIONS FROM ANNUAL TAX BILL IGRS
(SECTIONS V & VI IN QUARTERLY PAYMENT SYSTEM IGR)

V. ISSUANCE OF BILLS

This section applies to preliminary and actual tax bills.
[In semi-annual payment system IGR: This section applies to the actual tax bills and second payment notices.]

A. E-Billing

Property tax bills may be issued in an electronic form as set forth in this section. G.L. c. 60, § 3A(b).

1. Program Authorization – The collector's use of e-billing must be approved by the mayor or board of selectmen. The scope and duration of that approval may be decided locally.

2. Taxpayer Participation – Taxpayers must agree to receive their property tax bills in an electronic form. Participation must be completely voluntary. No taxpayer may be required to receive an electronic bill.

   Each taxpayer who wants to participate in the e-billing program must be informed and agree, in a written form, to the terms and conditions of the program. At a minimum, the program must require the taxpayer to:

   a. Provide the collector, in the manner and by the date prescribed by the collector, with an accurate e-mail address for e-billing purposes.

   b. Notify the collector, in the manner and by the date prescribed by the collector, of any change in e-mail address to be used for subsequent e-billing purposes.

   c. Accept electronic billing as the sole means by which the collector is legally required to give notice of the taxpayer's property tax obligations.

   d. Acknowledge any electronic bill issued to the e-mail address provided to the collector is a valid and properly issued property tax bill and failure to receive it does not alter the taxpayer's legal obligation to make payments, or file abatement or exemption applications, on time.

3. E-Bill Form and Content – The form and content of e-bills must be the same as the mailed bills and must meet all requirements set forth in these guidelines for property tax bills.

4. E-Bill Issuance – The bill may be issued in the e-mail message, as an attachment to the e-mail, or a link in the e-mail that allows the taxpayer to obtain it.

B. Bill Inserts

Information may be inserted in the same envelope or e-mail as the property tax bills as set forth in this section.

1. Property Tax Billing Information – The collector may insert property tax billing information. Property tax billing inserts are those advising taxpayers of tax billing and payment information such as (a) a new location for the collector's office, (b) collector's office hours, (c) payment options such as electronic payments, (d) different due dates because of later issuance of the tax bills than usual or (e) changes in tax payment systems (semi-annual to quarterly for example).

2. Consolidated Bills and Billing Information – The collector may insert bills for utility charges or fees as authorized by a consolidated billing by-law or ordinance, and information explaining adopted consolidated billing procedures. See Section IV-C below.

3. Non-political Municipal Information – The collector may insert non-political municipal informational material **if the insert (a) is approved by the mayor or board of selectmen and (b) does not increase the postage required to send the property tax bill by mail**. G.L. c. 60, § 3A(d). Non-political means information that does not advocate for, or seek to advance or influence a particular policy position or candidate. Municipal informational material means information that originates with the municipality and relates directly to municipal operations, services and programs.

C. Consolidated Billing

Bills for utility charges and fees may be included in the same envelopes or e-mail as the property tax bills as set forth in this section. G.L. c. 60, § 3A(c).

1. Program Authorization - Consolidated billing must be authorized by by-law or ordinance.

    a. Municipal Utility - The by-law or ordinance may allow one or more of the bills for the following municipal utility charges or fees to be included with property tax bills:
        - Water use.
        - Sewer use.
        - Solid waste disposal or collection.
        - Gas.
        - Electricity.
        - Other municipal utility.

b. Independent Water and Sewer Commission - If water and sewer service in the municipality is provided by an independent water and sewer commission established under G.L. c. 40N or a special act as a separate body politic and corporate from the municipality, the by-law or ordinance may also permit bills for water and sewer use charges assessed by the commission to be included with the property tax bills **if approved by vote of the commission.**

2. Bill Identification – The bill for each charge or fee must be separate and distinct from the property tax bills and from each other. Various means may be used, including but not limited to, making the bills different sizes or printing them on different color paper, distinctively captioning the bills or providing separate and distinctively identified attachments or links in e-mail.

3. Collection – Bills for charges or fees may be included with the property tax bills even if the customer is to remit payment for the particular charge or fee to the municipal board, officer or department assessing it, not the collector. The collector does not have to be a municipal collector charged with collecting all municipal bills for a municipality to use consolidated billing.

4. Assessed Ratepayer – The collector may only include bills for utility charges and fees assessed to and owed by the property owner being sent the property tax bill, *i.e.*, the assessed or current property owner shown on the property tax bill. See Section I-A-2 above. Bills for charges and fees assessed to tenants or others contracting for the service cannot be included in the property owner's tax bill. They must be sent to the assessed ratepayers.

5. Consolidated Billing Information - In the first year consolidated billing is used or changed, the collector must include a separate insert with all property tax bills to explain the new billing procedure to taxpayers. The collector may elect to include consolidated billing information with tax bills in other years, and if so, may include it as a separate insert, or as part of a property tax billing insert. See Section IV-A-1 above.

   Consolidated billing information advises taxpayers of (a) the utility bills being sent with their property tax bills and the means of distinguishing them, (b) the remittance and payment procedure for each bill, including, for example, whether payment for the charge or fee is to be sent to the collector or the municipal board, officer or department or independent commission that assessed the charge or fee, and (c) the changes, if any, made by the community in the billing schedule for a charge or fee in order to be able to the send the bills with the property tax bills.

VI. APPROVAL OF BILLS

Cities, towns or districts may print bills for mailing or prepare bills for electronic billing without the prior written approval of the Bureau of Municipal Finance Law, provided all bills conform to the minimum requirements for form and content established in this guideline. Only bills that meet these requirements may state "This form approved by Commissioner of Revenue."

Question: Can cities and towns send property tax or other bills by email?

TA Response: With the approval of the Municipal Relief Act on July 27, 2010 (c. 188 of the Acts of 2010), cities and towns are now authorized to issue property tax bills in electronic form. Section 54 of the Act amends M.G.L. C. 60 by adding new language to §3A that allows tax bills to be sent by email and other bills and nonpolitical information to be inserted with the mailing.

The local decision to allow issuance of the so-called "e-bills" rests with the board of selectmen in a town and the mayor in a city. There are two primary components to the authorization:

1) Like hardcopy bills, electronic property tax bills must be in a form approved by the Commissioner of Revenue and must meet the "content" requirements imposed by c.60, §3A, subsection (a), which are unchanged; and

2) The program must be voluntary. Taxpayers cannot be forced to receive an electronic bill.

The legislation encourages a paperless system where the only tax bill received by property owners would be an email copy. Savings would be realized through the elimination of printed bills and postage for mailings two or four times a year. To receive an electronic bill or notice, taxpayers must explicitly enroll and provide their email address to the collector.

In addition, municipal collectors are permitted to include, with the electronic property tax bill, other charges for water or sewer use, solid waste disposal or collection, or electric, gas or other utility services. These can only include charges that are authorized by ordinance or by-law and that are assessed by the city or town. The inserted bills or notices of payments due must be separate and distinct from the property tax bills. In the case where a separate commission oversees the water or sewer operation, it rather than the selectmen or mayor would authorize utility e-bills.

The authority previously granted to municipalities to include nonpolitical informational material in an envelope with the tax bill is now expanded. The inclusion of additional information with an email tax bill is permitted, but requires the approval of the selectmen or mayor.

In developing an electronic tax bill program, the municipal collector should work with local assessors and a technology advisor. Among other topics, consideration might be given to the following:

- **Enrollment**. Property owners should have the ability to enroll on-line at a dedicated town webpage. A verification mechanism must be built into the process. For instance, enrollment could be confirmed through a required return email acknowledgement by the property owner. The pertinent information could then be incorporated automatically into a data base. Over-the-counter enrollment or enrollment by mail is also an option and must include a written enrollment acknowledgement. Staff time would then have to data enter the information into the system or program.

- **Technology**. For tax bills, the assessors' appraisal system should allow property accounts, where owners have requested an electronic bill, to be flagged. The taxpayer accounts would remain in the commitment to the collector, but no hardcopy bill would be printed or mailed. A similar process should be developed for other types of bills that might be inserted with the electronic property tax bill. In each instance, the collector should have the ability to print a copy of the bill, if needed.

- **Legal**. At the time of enrollment to receive an e-bill, property owners should be required to, at least, acknowledge that:

  - they understand by enrolling they will not receive a bill in the mail or in any other hardcopy form;

  - they are responsible for the accuracy of the information provided;

  - they are solely responsible for reporting any changes to the information on file;

  - they are not relieved of the legal obligation to make timely payment if they fail to receive a tax bill, or any other bill, because of incorrect information;

  - they attest to the truth and accuracy of the information provided.

To assist municipalities further, the DLS Municipal Law Bureau in the process of drafting an Informational Guideline Release on the topic of e-bills.

Identity Theft: Start Protecting Your Community's Personal Information

Whether it's a lost thumb drive, a misplaced report or a computer network infected with malicious software, identity theft is a growing problem in Massachusetts and across the country. All too often we hear horror stories of organizations inadvertently exchanging sensitive information or losing vital records. The media now regularly reports on the loss of personal information by businesses, nonprofits and government agencies alike.

Data breeches can not only cost hundreds of thousands of dollars, but result in lost productivity as staff deal with resolving the issue. In the private sector, customers can quickly lose confidence in the ability of an organization to protect vital information, and take their business elsewhere.

In the public sector, cities and towns are not immune. Identity theft poses a serious problem that can damage the credibility of local government. Some recent reports of identity theft impacting Massachusetts municipalities include:

> An email with the social security numbers, names, and employee identification numbers was accidentally sent to department heads. Some of those emails were automatically forwarded to personal accounts and handheld devices.
>
> An envelope containing the social security numbers, addresses and dates of birth of individuals was mailed to a government agency. When it arrived, the envelope was opened and the contents were missing.
>
> A hacker infected a computer with a virus that tracked the keystrokes including security codes and passwords entered by an official. The information gathered was then used to transfer a considerable amount of funds overseas.

There is no question that cities and towns need to make a conscious effort to invest in methods that protect the public and the municipality when it comes to securing personal information. Examples of personal information include a resident's name in combination with a social security number, driver's license number or financial account information such as bank account or credit card numbers.

Massachusetts General Law (M.G.L.) Chapters 93, 93H and 93I establish comprehensive identity theft prevention measures for business and governmental entities. Although municipalities are exempt from certain regulations promulgated by the state as a result of these laws (201 CMR 17.00), other provisions relative to securing personal information apply

to cities and towns. Specifically, M.G.L. c. 93H includes prompt disclosure requirements when personal information is lost or stolen, while M.G.L. c. 93I sets standards for the disposal of records containing personal information.

So what can be done? To answer this, we outline a process for municipalities to begin protecting confidential information. This is by no means intended to be a comprehensive solution, but includes some immediate steps that cities and towns should take to identify and secure personal information. Also, at the end of this article we provide links to outside resources that provide additional information on implementing preventative identity theft measures.

1. *Designate a Point Person* – First, it is important to determine who will spearhead the initiative and coordinate the city or town's response to protecting personal information. The team leader will be responsible for coordinating access and information gathering among the various departments. The individual should be technically savvy, be able to communicate effectively and be comfortable working with stakeholders from across the organization.

2. *Assemble a Team* – Second, a team of no more than seven members should be formed with the responsibility to collect information and develop a security protocol. We suggest that representatives include someone from the information technology, human resources, finance, legal, and executive offices. Team members should become familiar with identity theft and the level of risk involved.

3. *Identify Personal Information* – Third, the team should compile a written inventory of personal information contained in municipal records. This comprehensive review will determine what constitutes personal information and where it resides within the town. This investigation should identify personal data in both paper and electronic format used by and/or stored by the municipality. Remember, in today's data driven world even photocopy machines store information locally on hard drives.

   Once complete, this document will be used to illustrate the magnitude of risk involved, and be incorporated as part of the overall security policy.

4. *Develop a Security Protocol* – Next, the team should develop, implement, maintain and monitor a comprehensive written security protocol to protect the community's personal information. A plan should include specific and clearly identifiable requirements for protecting confidential data maintained by a department. Although a number of policies are widely circulated on the web, a security plan generally addresses the collection of information, record access, controls, record retention and destruction, physical security, training, and reporting. A final work product should answer any questions related to the protection of personal information within the

municipality. At the end of this article we provide a link to a sample identity theft policy.

5. *React to a Breach* – Lastly, your city or town must react swiftly, and not hesitate to request outside assistance, if personal information is accidentally disclosed or deliberately stolen. We suggest that the team convene to complete an initial assessment of the breach, identifying how and what information might be affected.

   More importantly, however, the team must begin the process of notifying those who might be impacted, so they can begin steps to monitor their accounts for any irregularities. Under M.G.L. municipal officials have the legal obligation to notify any resident affected by the release of personal information, as well as the attorney general and the director of consumer affairs and business regulations.

   Once the team is confident that appropriate steps have been taken to identify, notify and resolve the issue, we recommend it complete a review to determine how future breaches can be prevented and what additional measures may be warranted.

To better understand identity theft, the potential impact to your community, and ways to assist your city or town in protecting confidential information, we provide the following links.

M.G.L. c. 93H: www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h

M.G.L. c. 93I: www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93I/

Department of Revenue, City & Town: http://www.mass.gov/Ador/docs/dls/publ/ct/2008/may08.pdf. Link includes a May 2008 article on Identity Theft Prevention by Gary A. Blau, Esq. Municipal Finance Law Bureau.

United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov/cas/tips/. Link includes general information about cyber security, including protecting passwords, understanding anti-virus software and firewalls, as well as recognizing, avoiding and preventing threats.

Multi-State Information Sharing and Analysis Center (MS-ISAC): www.msisac.org/localgov/. Link provides a whole host of resources including guidelines for backing up information, internet and acceptable use policy templates and getting started guides.

Commonwealth of Massachusetts Information Technology Division: www.mass.gov/itd. Link offers various templates, and an information security policy guide

Legal

Identity Theft Prevention

Gary A. Blau, Esq., Municipal Finance Law Bureau

On August 2, 2007 the legislature, with the approval of the governor, passed Chapter 82 of the Acts of 2007, "An Act Relative to Security Freezes and Notification of Data Breaches," otherwise known as the Identity Theft Prevention law. The act amends M.G.L. Ch. 93 and adds M.G.L. Ch. 93H and 93I to establish comprehensive identity theft prevention measures for business and governmental entities. Except for the new Chapter 93I providing for the distribution and destruction of records, which was effective February 3, 2008, the remainder of the law was effective October 31, 2007.

Under amendments to M.G.L. Ch. 93 (Regulation of Trade), consumers may secure credit freezes to prevent new accounts from being fraudulently created in their name. Under the new M.G.L. Ch. 93H, businesses and governments must promptly notify affected residents of the commonwealth and state agencies when the residents' personal information is lost or stolen. Personal information includes the customer's or resident's name in combination with a Social Security, driver's license or financial account number. It does not include any data found in records which are otherwise public. The attorney general may bring an action to remedy violations.

Governmental entities that maintain and store personal information, but do not own or license the data, including agencies, departments, boards and commissions of local governments, must notify as soon as practicable the owner or licensor of the information and cooperate with the owner or licensor when the data has been breached. Governmental entities that own or license the personal information must notify as soon as practicable residents of the commonwealth whose data has been breached, the attorney general, the director of consumer affairs and business relations, and any consumer reporting agencies and state agencies identified by the director when the personal information has been breached. M.G.L. Ch. 93H, §3. The statute does not define "owner or licensor," but the terms appear to include a local government entity that acquires the information directly from the data subject for the agency's own use. Any required notice may be delayed if a law enforcement agency determines that providing the notice may impede a criminal investigation, notifies the attorney general, in writing, and informs the agency reporting the breach of the determination.

The new M.G.L. Ch. 93I sets standards for the disposal of records containing personal information by businesses and governments.

The new M.G.L. Ch. 93I sets standards for the disposal of records containing personal information by businesses and governments. Personal information for purposes of this chapter includes the customer's or resident's name in combination with a Social Security, driver's license or financial account number or a biometric indicator. "Biometric indicator" is not defined, but presumably includes fingerprints, DNA information, dental X-rays, retina scans and other such identifying information. Documents or other records containing personal information must be redacted, burned, pulverized or shredded. Electronic and other media must be destroyed or erased so that personal information cannot be read or reconstructed. Governmental agencies are specifically authorized to contract with third party vendors for the disposal of information, and those vendors will be required to safeguard the data while complying with the disposal provisions of the chapter. Violators are subject to a civil fine of not more than $100 per data subject affected up to a maximum $50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover penalties and may bring an action to remedy violations.

The director of consumer affairs and business regulation is responsible for setting regulations for how businesses must protect personal information to prevent data breaches. The business regulations may be found at 201 CMR 17.00 at the Office of Consumer Affairs and Business Regulation website, www.mass.gov/oca. These regulations apply to "persons" who own, license, store or maintain personal information about a resident of the commonwealth, but a "person" does not include the commonwealth, its agencies and political subdivisions.

The supervisor of public records in the secretary of state's office, with the advice and consent of the Information Technology Division as to technology standards, is charged with establishing rules and regulations designed to protect the personal information of commonwealth residents that is owned by or licensed for commonwealth executive offices, agencies, departments, boards, commissions and instrumentalities of an executive office and any authority created by the state legislature. The supervisor has not yet issued rules and regulations, but has initially determined that its guidance will be limited to commonwealth executive office and other state agencies and not to local governments, because the statute does not grant the supervisor that authority.

continued on page 9

Identity Theft Prevention continued from page 3

While the regulations issued by the director and supervisor do not apply to cities, towns, districts, counties, regional school districts or other local government, they can provide general advise and guidance to local governments as they prepare their own ordinances, bylaws, rules and regulations or guidelines to safeguard personal information and address any security breach.

Local government departments likely to have personal information covered by the law include police, assessing, collection and treasury departments that acquire Social Security numbers from individual residents, including subjects of investigations, applicants for exemption, delinquent taxpayers or ratepayers and employees. Each department should devise a plan to safeguard and destroy the data when no longer required to be kept by law, and to determine when a breach has occurred and a plan of action in that event.

Safeguarding and disposing of information retained electronically provides particularly difficult challenges for local governments, requiring enhanced encryption, limiting access to employees with a need to know by password or pin restrictions, monitoring outgoing e-mail with Social Security number detecting software and similar mechanisms. Use of experts in protection and disposal of electronic personal information may be necessary if the local government entity does not have such expertise on staff. ■

Forest, Farm and Recreational Chapter Lands continued from page 4

sessors. It cannot include any other land held for the production of income or land under a permanent conservation restriction. M.G.L. Ch. 59, § 2A(b).

Acceptance Procedure

Local acceptance of any of the new local option statutes requires a majority vote of the municipality's legislative body, subject to the municipal charter. M.G.L. Ch. 4, § 4.

The acceptance vote should be made before the January 1 classification date for the fiscal year the option is intended to first take effect so that the assessors can classify the land in a timely fashion. The vote may be taken later, however, so long as the tax rate for that year has not been set. To avoid questions about the effective date, all acceptance votes should expressly state the fiscal year the option will first apply. DLS also recommends that a separate vote be taken for each optional statute the city or town wants to accept. The following or similar language may be used for the acceptance vote:

> VOTED: That the city/town of XXXXXX accept (M.G.L. Ch. 61, § 2 A/M.G.L. Ch. 61A, § 4A/M.G.L. Ch. 61B, § 2A), which taxes classified (forest/farm/recreational) land as open space instead of commercial property, to be effective for taxes assessed for any fiscal year beginning on or after July 1, XXXX.

The city or town clerk must notify the Municipal Data Management/Technical Assistance Bureau of the acceptance of any of these local option statutes. The notification should be made as soon as possible after the vote on the acceptance form found on the Municipal Data Bank Local Options page of the DLS website.

Once accepted, the assessors must assign the classified forest, farm or recreational land to the open space class even if they are not classifying any other land as open space or the classified land does not precisely fit the written criteria they established for open space classification.

A city or town may revoke its acceptance of any of the local option statutes, but must wait at least three years after the statute was accepted to do so. Revocation is also by vote of the legislative body subject to local charter. M.G.L. Ch. 4, § 4B. The following or similar language may be used:

> VOTED: That the city/town of XXXXXXX revoke its acceptance of (M.G.L. Ch. 61, § 2 A/M.G.L. Ch. 61A, § 4A/M.G.L. Ch. 61B, § 2A), which will result in the taxation of (classified forest/farm/recreational) land as commercial instead of open space property, to be effective for taxes assessed for any fiscal year beginning on or after July 1, XXXX.

Future articles will look at other changes Chapter 394 made in the chapter land statutes. ■

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Section:
17.01: Purpose and Scope
17.02: Definitions
17.03: Duty to Protect and Standards for Protecting Personal Information
17.04: Computer System Security Requirements
17.05: Compliance Deadline

17.01 **Purpose and Scope**

(1) Purpose
This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope
The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: **Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal information, 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.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

17.03: **Duty to Protect and Standards for Protecting Personal Information**

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:
(a) Designating one or more employees to maintain the comprehensive information security program;
(b) Identifying and assessing reasonably foreseeable internal and 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, including but not limited to:
1. ongoing employee (including temporary and contract employee) training;
2. employee compliance with policies and procedures; and
3. means for detecting and preventing security system failures.
(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.
(e) Preventing terminated employees from accessing records containing personal information.
(f) Oversee service providers, by:
1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.
(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.
(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
(i) Reviewing 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.
(j) Documenting 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.

17.04: **Computer System Security Requirements**

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a

security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:
(1) Secure user authentication protocols including:
(a) control of user IDs and other identifiers;
(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
(d) restricting access to active users and active user accounts only; and
(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
(2) Secure access control measures that:
(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
(5) Encryption of all personal information stored on laptops or other portable devices;
(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: **Compliance Deadline**

(1)Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

REGULATORY AUTHORITY

201 CMR 17.00: M.G.L. c. 93H

Related pages:

Records Conservation Board

State Records Center

Public Records Division

Back to:

Records Management Home

Massachusetts Archives Home

Secretary of the Commonwealth Home

SPR Bulletin NO. 1-08

TO: (1) Executive offices and any agencies, departments, boards, commissions and instrumentalities within an executive office; and (2) any authority created by the General Court.
SUBJECT: **Security Breach Protections**
EXPIRATION DATE: Given the dynamic nature of this issue, records custodians are advised to regularly refer to the websites of the Supervisor of Records and the Information Technology Division for updates. This Bulletin remains in effect until superseded.
PURPOSE: This Bulletin provides requirements designed to safeguard the personal information of residents of the Commonwealth that is owned or licensed by certain agencies of government.

BACKGROUND:
It is the intent of the Secretary of the Commonwealth to ensure that personal information about Massachusetts residents is protected. To that end, the purpose of this Bulletin is to encourage the agencies to which this Bulletin applies to provide reasonable security for that information. As authorized by Section 2B of Chapter 93H, the Supervisor of Records, with the advice and consent of the Information Technology Division, is authorized to issue this Bulletin concerning the safeguarding of personal information of Massachusetts residents. The following provisions will apply to: (1) executive offices and any agencies, departments, boards, commissions and instrumentalities within an executive office; and (2) any authority created by the General Court.

FINDINGS:
1. Identity theft is an area of great concern that faces the residents of the Commonwealth. The Office of the Secretary has been charged by the Legislature, with the advice and consent of the Information Technology Division, to issue provisions to guard against anticipated threats or hazards to the security or integrity of certain personal information on file, maintained or otherwise under the control of certain state agencies, and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the Commonwealth.

2. Personal information is defined in Section 1 of Chapter 93H as a resident's first name and last name or first initial and last name in combination with any 1 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.

ACTIONS:

1. An agency to which this Bulletin applies shall establish, execute, and manage an inclusive, written information security program that applies to any records under their custody or control containing personal information, as defined in Section 1 of Chapter 93H. The security program should take into consideration the legal requirements for the retention and destruction of the records at issue. Additionally, the records management policy should develop procedures that address the identification, retention, retrieval, ultimate disposition or destruction of and access to these records containing personal information.

2. An agency to which this Bulletin applies shall provide guidance to employees regarding how to identify and maintain information that contains personal information.

3. An agency to which this Bulletin applies shall take all reasonable steps to destroy, or arrange for the destruction of a Massachusetts resident's records within its custody or control containing personal information which is no longer to be retained by the agency in compliance with the destruction provisions of Section 2 of Chapter 93I, the Records Conservation Board and/or the Supervisor of Records, agency business needs, or the requirements of any other Federal or state records retention requirement including, without limitation, rules of civil or criminal procedure.

4. An agency to which this Bulletin applies that owns or licenses personal information about a Massachusetts resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

5. An agency to which this Bulletin applies that discloses personal information about aMassachusetts resident pursuant to a contract with a nonaffiliated third party executed after implementation of this Bulletin shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

6. As required by Section 3(c) of Chapter 93H, an agency within the Executive Department must provide written notification of the nature and circumstances of a security breach or unauthorized acquisition or use of personal information to both the Information Technology Division and the Division of Public Records. The agency is required to comply with all policies and procedures adopted by the Information Technology Division pertaining to the reporting and investigation of such an incident.

7. The written notification, at minimum, must contain information concerning:

a) The nature of the breach of security or unauthorized acquisition or use of personal information;

b) The number of individuals affected;

c) Actions taken to address the security issue;

d) Measures to be implemented to prevent similar security issues;

e) Contact information for an individual at the agency who can provide further information concerning the security issue, if necessary.

8. An electronic communication will satisfy the requirement for written notification. See G.L. ch. 110G. The Information Technology Division requests that notification, pursuant to Section 3(c) of Chapter 93H, is provided electronically via an email sent to Information Technology Division's Chief Information Officer and copied to the Information Technology Division's Security Officer and General Counsel, rather than via paper letter.

9. The exemptions to the Public Records Law shall apply to the records created pursuant to Chapter 93H. Please note, these exemptions from disclosure are strictly and narrowly construed. Agencies are encouraged to refer to Chapter 4, Sections 7(26)(a-q) in order to properly apply the exemptions in the manner necessary to maintain the integrity and security of these records. Questions regarding this Bulletin, as well as notifications pursuant to Section 3(c) of Chapter 93H should be directed to:

Supervisor of Records
Public Records Division
1 Ashburton Place, Room 1719
Boston, MA 02108
Phone: 617-727-2832
Fax: 617-727-5914
www.sec.state.ma.us/pre

Information Technology Division
One Ashburton Place, Room 804
Boston, MA 02108
Phone: (617) 626-4448
Fax: (617) 626-4459
www.mass.gov/itd
