Massachusetts Passes Law Regarding Disposition and Destruction of Records Containing Personal Information

---

On February 3, 2008, a new Massachusetts law, G.L. c. 93I, went into effect that sets forth minimum standards for the disposition and destruction of records containing personal information relating to residents of Massachusetts. MIT is subject to this law and is therefore required to comply with it, effective immediately.

The law applies to any document, whether electronic or in paper form, that contains personal information. "Personal information" is defined to include the following:

> **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 the resident:—**
>
> **(a) Social Security number;**
>
> **(b) driver's license number or Massachusetts identification card number;**
>
> **(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; or**
>
> **(d) a biometric indicator.**

Under the new law, if a paper document containing personal information is to be disposed of, it **"shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed."** If electronic media or other non-paper media containing personal information are to be disposed of, they **"shall be destroyed or erased so that personal information cannot practicably be read or reconstructed."**

The law does not further define what it means for electronic information to be destroyed or erased so that it "cannot practicably be read or reconstructed," nor are there any regulations or cases interpreting that phrase, but simple deletion of an electronic file containing personal information is probably not sufficient. In the absence of further explanation, one resource that is available is the "Guidelines for Media Sanitization" published by the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") (NIST Special Publication 800-88). The NIST Guidelines can be found at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf. In addition, IS&T has published a page on its website that discusses options for media sanitization: http://web.mit.edu/ist/topics/security/media_sanitizing1.html.

Currently, the law does not set forth any requirements for when, or under what circumstances, documents containing personal information must be disposed of or when

they must be kept. Rather, the only express requirement is that, when such documents are disposed of, they must be disposed of in accordance with these minimum standards.

Under a separate portion of the new law, G.L. c. 93H, entities such as MIT are also required to provide notification to Massachusetts residents in the event of certain data security breaches involving personal information.

In light of this and other laws, as well as the increasing risk of identity theft in today's digital age, MIT departments are advised to reevaluate their use and retention of personal information and to take steps to protect against the inadvertent loss or disclosure of such information. Although there is no "one size fits all" approach to the handling of personal information, relevant considerations include:

- Ensuring that people who have access to personal information understand their responsibilities, including through regular training, particularly for new or temporary staff.
- Collecting and retaining only such personal information as is reasonably necessary for the legitimate purposes of the department.
- Limiting the use of laptops and other portable media or devices to store personal information.
- Storing paper documents with personal information in secure/locked locations.
- Restricting access to personal information to those individuals who reasonably need access to perform their job duties.
- Limiting the use of e-mail and interoffice mail to transmit personal information.
- Immediately reporting potential data security breaches involving personal information.

For assistance in developing a local information policy in your department, contact pii-protect@mit.edu. MIT has also established a response team in the event a data security breach occurs at the Institute. If you believe a breach has taken place, contact infoprotect@mit.edu. If you have questions about this new law, contact Jay Wilcoxson in MIT's Office of the General Counsel at 617-253-7724 or jaren@mit.edu.