INFORMATION STEWARDS & STEWARDSHIP COMMITTEE

INFORMATION STEWARDS PROGRAM
You can find your Information Steward, and stewards for other locations by accessing the following website:

http://go.tufts.edu/infostewards

INFORMATION STEWARDSHIP COMMITTEE
The Information Stewardship Committee serves as an advisory body to formulate guidance and advice on best practices and strategies for good information stewardship.

http://go.tufts.edu/isc

FOR ADDITIONAL INFORMATION
http://go.tufts.edu/guardit

Overview of Massachusetts Data Privacy Regulations

This program was collaboratively developed by Audit and Management Advisory Services, Digital Collections and Archives, Human Resources, University Information Technology, and University Counsel.

March 2010
OVERVIEW OF LEGISLATION

Over the past two years, the Commonwealth of Massachusetts has enacted laws and regulations to protect the Personal Information (as defined below) of its citizens. These laws and regulations, designed to protect against identity theft, apply to all persons and departments within Tufts that store, maintain, or use Personal Information. This handout provides an overview of the applicable Massachusetts laws and regulations, general requirements, and helpful resources where you can receive more information.

Tufts University takes its data privacy responsibilities seriously and is continually working to ensure that the appropriate safeguards are in place to protect the Personal Information of students, faculty, staff, alumni, and other members of the Tufts community.

PERSONAL INFORMATION

The Commonwealth defines Personal Information as the first name (or first initial) and last name of any Massachusetts resident, in combination with any one of the following:

- Social Security Number
- State ID Number (e.g. drivers license number)
- Financial Account Number (e.g. credit card number)

REQUIREMENTS OF MASSACHUSETTS LAWS AND REGULATIONS

Under Massachusetts General Laws Sections 93H and 93I, an organization that maintains or has access to Personal Information is required to:

1. Take appropriate steps to protect such Personal Information;
2. Notify the Attorney General when such Personal Information is exposed to unauthorized access or unauthorized usage; and
3. Use secure methods to destroy unneeded Personal Information.

The state regulations implemented under Section 93H require that organizations maintaining Personal Information adopt an Information Security Program that monitors for unauthorized usage and access. In addition, the regulations outline technical and operational requirements for protecting both electronic and physical records that contain Personal Information.

WHAT YOU NEED TO DO

1. KNOW YOUR INFORMATION STEWARD

   In order to facilitate effective programs in our distributed environment, Information Stewards have been appointed within all schools, divisions, and major departments. These individuals are charged with understanding how Personal Information is used and helping to ensure that the proper safeguards are in place.

2. DETERMINE IF YOU USE PERSONAL INFORMATION

   If you collect or use Personal Information, or hire an outside contractor to do so, the University is legally obligated to protect such information. You are not alone in this task; the Information Steward within your school, division, or department can work with you to ensure that the proper safeguards are in place. Therefore, if you use Personal Information, either in electronic or physical form, please contact your Information Steward today.

3. TECHNICAL REQUIREMENTS FOR ELECTRONIC DATA

   Computers that contain personal information must meet the following requirements. Your Information Steward, in conjunction with your FSP or support person, will work with you to ensure that you comply with these and other applicable technical requirements:
   1. Up-to-date anti-virus software with current signatures
   2. Installation of all current security patches and updates
   3. Hardware or software-based firewalls
   4. Whole disk encryption for laptops
   5. Strong passwords and unique accounts when accessing personal information
   6. Encryption when transmitting personal information over the Internet
   7. Encryption of any personal information residing on a mobile device (e.g. mobile phone, USB memory stick, CD-ROM, etc.)

   If you are a system or application administrator, please consult with your designated Information Steward. The regulations maintain specific requirements for servers and applications.

4. SAFEGUARDS FOR PHYSICAL DATA

   Paper records are just as important as electronic records and must be appropriately secured. Consult with your Information Steward to determine if your paper records are appropriately placed in locked and secured containers.