

GET S.M...A.R.T!

How to Identify, Maintain and Safeguard **Personal Information**
at our State Institutions of Higher Education

Get S.M...A.R.T!

Security

Matters ...

Adapt ... To new policies, procedures and regulations

Respect ... The Privacy of Personal Information

Think! Before accessing or disseminating information

Introduction

Whether you are working at an Institution of Higher Education or attending one, you may come into contact with confidential information. Some is your confidential data, some belongs to others. Everyone has a role in protecting personal information or personal data. It is critical to be aware of the policies, guidelines and laws that govern how we use, share and protect that data.

What governs how the institution protects data?

- State and Federal statutes and regulations regarding privacy and security
- Contracts between state agencies and data providers (e.g., Social Security Administration)
- MA Information Technology Department (ITD) Security Policies, Standards and Guidelines
- Our local Security Policies and Standards

What would you do for a candy bar??



- A 2007 survey found that more than **70% of people would reveal their computer password in exchange for a bar of chocolate.**
- **34% of respondents volunteered their password** when asked without even needing to be bribed.
- A second survey found that **79% of people unwittingly gave away information** (when questioned) that could be used to steal their identity.

Consequences of unauthorized use ... or access of **personal information**

- **Identity Theft**

- Many victims claim to forfeit something like \$2,000.00 to \$15,000.00 in lost wages as a result of identity theft.
- Victims have had to declare bankruptcy because of an identity theft that destroys their credit and ability to work.

- **Mitigation Costs**

- 230 billion dollars are lost each year, world wide, as a result of identity theft

- **Staff/System/Agency Downtime**

- **Loss of Public Confidence and Reputation**

- **Legal Issues**

- Businesses report that they spend an average of \$15,000.00 or more in costs for an identity theft case

How is Personal information defined under MGL 93H, EO504 and FIPA?

- M.G.L 93H defines **Personal Information** as a **resident's first name and last name** (or **first initial and last name**) in combination with one or more of the following:
 - Social Security number;
 - Driver's license number or state issued ID number
 - Financial account number
- Any information which can be readily associated with a particular individual
 - Name
 - Identifying number
 - Mark (like a photo)
 - Description
- Institutions seek to protect personal information and to prevent an unauthorized individual from:
 - Stealing some one's identity for an unlawful or unauthorized purpose.
 - Gaining unauthorized access to information that may cause embarrassment to the organization or an individual.
 - Using unauthorized access to disrupt or damage the integrity of enterprise data sources.

Exceptions:

- × Information contained in a Public Record
- × Intelligence information, evaluative information, or criminal record information which is covered by the CORI Act (Criminal Offender Record Information)

Contractual security requirements

- **FERPA** (**F**ederal **E**ducation **R**ights and **P**rivacy **A**ct)
- Payment Card Industry (**PCI**) Data Security Standards
 - Certain data security standards mandated by the credit card industry for all Commonwealth entities that process, transmit, or store cardholder data
- Social Security Administration Information Exchange Agreement
 - Governs the transmission of data files received from and sent to the Social Security Administration
- **HIPAA** (**H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct)

Examples of Personal Information:

- Student/Employee Record Information
- Student/Employee ID
- Health Service or Campus Police records
- Credit Card Information
- Driver's License
- Social Security card (Name and SSN)

Non-electronic ways that **Personal Information** can be stored (or shared)

- What?
 - Reports
 - Letters
 - Faxes
 - Printouts
 - Memos
 - Notepads
 - Sticky Notes
- Where/How?
 - File Cabinets
 - Desks
 - Printer/Fax Trays
 - Personal effects (briefcases and pockets!)
 - RECYCLE BINS!
 - Posted test grades (doors/walls)
 - Class rosters
- When you're talking...
 - Phone Calls
 - Meetings/Conversations

Electronic ways that **Personal Information** can be stored (or shared)

- **Personal Devices**

- Computers
- Laptops
- PDAs
- Smart phones
Cell phones
- Flash drives

- **Infrastructure**

- Email
- Voicemail
- Local and network drives
- Servers or remote hosts
- Equipment in storage, awaiting disposal
- Backup tapes
- Applications that collect or use **Personal Information**

Systems/Offices that MAY contain Personal Information

- (Depending on location...) Sungard SCT Banner, PeopleSoft, Jenzabar, Colleague Datatel, Raisers Edge, etc.
- Campus Police Logs
- State reports through Warehouse and MMARS
- Campus-developed reporting applications
- Student Health Clinics
- Judicial Offices
- Advancement/Development/ Alumni
- Housing Records
- Fitness/Wellness Centers

Laws and Regulations

MGL 66A

FIPA creates a non-disclosure requirement of personal data when such information is not subject to disclosure under the Freedom of Information Act

MGL 93H/93I

Outlines how agencies provide notice in the event of unauthorized access, use or breach of Personal Information

EO 504

Requires agencies to adopt, develop and a program to ensure the security, confidentiality and integrity of Personal Information

Promotes the importance of uniform policies and standards across state government through approved, written information security programs

Laws and Regulations

Red Flags Rule

Requires all organizations (subject to the legislation) to develop and implement a formal, written and revisable “Identity Theft Prevention Program” to detect, prevent and mitigate identity theft.

PCI-DSS Compliance

Mandatory compliance program resulting from a collaboration between the credit card associations to create common industry requirements for cardholder data.

Campus Information Security Program

THE GOAL:

- Adopt and implement the “*maximum feasible measures*” reasonably needed to ensure the security, confidentiality and integrity of Personal Information

Under the security policy, ALL employees (*including contractors*) must:

- **Collect the minimum quantity of personal information** reasonably needed to accomplish the legitimate purpose for which information is being collected.
- **Securely store and protect Personal Information** against unauthorized access, destruction, use, modification, disclosure and loss
- **Disclose** Personal Information and data *only on a need-to-know basis*
- **Destroy** Personal Information and data *as soon as it is no longer needed or required* to be maintained under state or federal law
- **Comply** with the College’s administrative, technical and physical safeguards and policies for Personal Information and with relevant Federal and State privacy and security laws and regulations

How does this impact my work?

Collect a minimum of information

- If you don't need it, don't ask for it. ONLY access information necessary for the proper performance of your job.
- Rethink current processes

Disclose Personal Information on a need-to-know basis

- If you receive a request for personal information outside the normal course of business, escalate the request before responding
- Watch out for...
 - Non-authorized persons seeking information
 - Phishing emails
 - Shoulder Surfing (*someone looking over your shoulder while you are at your computer*)
 - Impersonation via email or phone solicitations

Destroy Personal Information when no longer needed.

- Consider the following before destroying any record
 - Active litigation
 - Records retention requirements for certain programs (HIPAA, Records in Common Schedule, email retention policies, etc.)

Methods Of Destruction

- Shred paper that contains personal information
- Computers, mobile devices - ensure proper deletion of files, destroy media and obtain a Certificate of Destruction

How does this impact my work?

- At Security Desks/Reception Desks/Information Desks - HAVE VISITORS SIGN IN and keep a record
- Issue Access ID s in critical areas and do not allow access without ID and authorization
- Lock file cabinets in offices that maintain Personal Information
- Do not leave Personal Information unattended in a non-secure environment, such as on desktop, in communal meeting spaces, in a printer tray or fax machine or on a sticky note in plain sight!
- Keep secure spaces SECURE!
 - Don't prop open doors or allow non-authorized person entry
 - In critical spaces, monitor with security cameras
- Only discuss Personal Information when appropriate to performing a job function in private locations (not elevators, cafeterias or hallways).
- Use privacy screens on computers if your monitor can be publicly viewed.

Student Employees...are you helping them to understand the importance of Personal Information

How does this impact my work?

- **System Security**

- Consider: Each network device is an “entry point”
- Employee desktop computers:
 - Even if you only use your office computer for email, that computer is part of your campus’s network and is related to YOUR identity on the network
- Publicly accessible computers/kiosks on campus
 - Ensure that they are used appropriately
 - Don’t walk away without logging off
 - Never allow anyone to use your login/password

Procedures and Policies

- Comply with your campus **Acceptable Use Policy**
- Do not access or disseminate Personal Information *unless required by your job*
- **NEVER, Ever, EVER share your password**
 - An employee of the college's Technology department may require you to present a password to perform service - CHANGE IT when he/she is finished
 - Technology employees do not ask you to provide your password via email request. Promptly notify your technology department if you suspect a password has been compromised
- Comply with the password complexity and expiration policies
- Log off, lock the keyboard, or lock the desktop when you step away from your computer
- All mobile devices **MUST** be encrypted
- Comply with application-specific security requirements
- Use resources appropriately. Do not store Personal Information in non-secure applications

Conclusion

- **Everyone is responsible for safeguarding personal information!**
- THINK before accessing or transmitting personal information
- Treat all personal information as if it was your own
- Do not release any personal information to anyone outside the college without first vetting through a common-sense internal process
 - Check with your manager
 - All legal requests get routed through a legal process and should be handled with the assistance of the institution's lawyers
 - Follow all privacy and security policies
 - Work with your manager to determine what responsibilities you own
- By doing all of these things, you are protecting yourself and others.

Links

MGL 93H: Massachusetts Data Breach Notification Law

<http://www.mass.gov/legis/laws/mgl/gl-93h-toc.htm>

Executive Order 504

<http://www.mass.gov/?pageID=afhomepage&L=1&L0=Home&sid=Eoaf>

201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth

<http://www.mass.gov/?pageID=ocahomepage&L=1&L0=Home&sid=Eoca>

Red Flags Rule

<http://www.ftc.gov/redflagsrule>

Massachusetts Records in Common

<http://www.sec.state.ma.us/arc/arcrmu/rmurds/adminandpersonel23-89.pdf>

Statewide Records Retention

<http://www.sec.state.ma.us/arc/arcrmu/rmuidx.htm>

PCI Compliance

<http://www.pcicomplianceguide.org>

Credits

This presentation was created by the **Information Security Committee**, comprised of the state colleges, community colleges and the university system. Many thanks to **Kristin Gronberg**, Salem State College; **Sherry Horeanopoulos**, Fitchburg State College; **Susan Hughes**, Mount Wachusett Community College; **Gene Kingsley**, Holyoke Community College; **Deb Moschella**, Framingham State College; **Jack Reardon**, Worcester State College;