Recent Data Breaches

Craft Store Michaels Confirms Data Breach Affecting 2.6 Million Credit Cards

By Ashlee Kieler  April 18, 2014

University of Maryland Reports 2nd Data Breach in 4 Weeks

Thursday, Mar 20, 2014 | Updated 5:39 PM EDT

Report: Utah's health data breach was a costly mistake

South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations

BOSTON – South Shore Hospital has agreed to pay $750,000 to resolve allegations that it failed to protect the personal and confidential health information of more than 880,000 consumers. Attorney General Martha Coakley announced today that the investigation and settlement resulted from a data breach reported to the AG’s Office in July 2010 that included

"WE TAKE THIS MATTER VERY SERIOUSLY AND ARE WORKING WITH LAW ENFORCEMENT TO BRING THOSE RESPONSIBLE TO JUSTICE."

GREGG STEINHAFEL
TARGET CHAIRMAN, PRESIDENT AND CEO
Data Types Targeted

• PHI – Private Health Information

• PII – Personally Identifiable Information (SSN)

• Protected Student Records

• Sensitive – Payroll Information, etc.
Protecting Privacy

Privacy: freedom from unauthorized & unwarranted intrusion; a protection that applies to the person.

Employees of UMMS have an obligation to protect the confidentiality of the data used and stored at UMMS, to protect individuals’ privacy.
Sources of Data Protection Requirements

- Statutes and Regulations
- Contracts
- Business Associate and Data Use Agreements
- Grant Awards
- Research Agreements
- IRB Approvals
Privacy Protection Laws

**HIPAA**
Privacy and security requirements to protect the confidentiality and integrity of health information and provide individuals rights to their information.

**GINA**
Prohibits discrimination in health coverage and employment based on genetic information.

- **MGL c. 70G**
  Protects genetic information from disclosure

**FERPA**
Purpose is to ensure educational records are kept private and guarantee access to these records by parents.

**MGL c. 93H**
Requirements to safeguard Personal Information of and to provide consumer notice to Massachusetts residents for the breach of security.

**Privacy Act of 1974**
Federal fair information practices governing collection, use and disclosure of personally identifiable information by federal agencies.

**Common Rule**
Rule of ethics regarding biomedical and behavioral research involving human subjects in the United States.

**Red Flags Rule**
Created to help prevent identity theft.

**FIPA**
Mass fair information practices act protecting personal data held by state entities and their contractors.

**UMASS Medical School**

*Confidential*
Compliance is Essential

Compliance with federal and state laws is essential for:

• Integrity of the information; research; client relations
• Reputation of the University
• Protection from liability and penalties

As a UMMS workforce member, you have a responsibility to maintain the highest standards of professional conduct.

If you suspect or become aware of a violation of privacy, report it to your supervisor immediately.
Minimum Necessary

• Collect, Access, Use and Disclose only the minimum necessary to do your work
• Access only information for which you are authorized to perform you work
• Do not remove confidential information from the work place unless authorized
• Adhere to information security requirements – can’t have privacy without security
1st Line of Defense – Passwords!

Passwords must be 8-14 characters long and contain three of the four of the following character types:
✓ Lower case characters
✓ Upper case characters
✓ Special characters
✓ Numbers

Your password cannot contain part of your name or be any of the previous 10 passwords.

Passwords Should Never Be Shared

University of Massachusetts Medical School
Information Services
Confidential
Forget your Password?

Visit inside.umassmed.edu

Password Self Service – Questions/Answers to reset your password yourself! Make sure to log in on your first day and set it up!
Focus: Healthcare

This can be often attributed to employee carelessness.

These breaches create MAJOR RISKS for patients including personal health facts being disclosed, financial identity theft and medical identity theft.

<table>
<thead>
<tr>
<th>Type of Device</th>
<th>Compromised or Stolen</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Drive</td>
<td>13%</td>
</tr>
<tr>
<td>Smartphone</td>
<td>24%</td>
</tr>
<tr>
<td>Notebook</td>
<td>2%</td>
</tr>
<tr>
<td>Tablet</td>
<td>18%</td>
</tr>
<tr>
<td>Desktop/laptop</td>
<td>38%</td>
</tr>
<tr>
<td>Server</td>
<td>5%</td>
</tr>
</tbody>
</table>

* Source: Medicalnewstoday.com and Backgroundcheck.org
Mistakes & Prevention

Don’t - Store information on a laptop

Don’t - Store information on a USB drive (portable device)

Do – Store it on a network drive!
Focus: Healthcare

What are the primary causes of breaches?

Common reasons include:

- **46%** A lost or stolen computing device
- **42%** Employee mistakes or unintentional actions
- **42%** Third party snafus
- **33%** Criminal attack
- **31%** Technical systems glitch
- **14%** Malicious insider
- **8%** Intentional non-malicious employee action

These breaches were discovered by:

- **52%** audit/assessment
- **47%** employee detected
- **36%** patient complaint

*Source: Medicalnewstoday.com and Backgroundcheck.org*
Suspect a Security Breach?

Normal Business Hours

Customer Service Help Desk

All IT Service requests can be submitted through the Help Desk.

Phone: 6-UMHD or (508) 856-8643 » Fax: (508) 856-2440
Email: umwhelpdesk@umassmed.edu » Walk-In Locations

Emergency Notification System • HR Direct • Manage Outlook Profile • UMass VPN

Stolen Laptop – Nights / Weekends

How to Contact the Department of Public Safety

Individuals may contact the Department of Public Safety the following ways:

• Speak directly to a police officer on campus.
• Call 856-3296 from a public pay phone or ext. 6-3296 from any telephone extension on campus.

Questions? Email ITSecurity@umassmed.edu
Questions?

• Create a strong password

• Know where you’re storing sensitive information

• Report any incidents