Protecting Health Information in the Commonwealth

Office of Attorney General
Martha Coakley
October 25, 2012

©2012 Office of Massachusetts Attorney General Martha Coakley

Massachusetts Data Security Law in the HealthCare Context

©2012 Office of Massachusetts Attorney General Martha Coakley
Massachusetts Data Security Law

- M.G.L. c. 93H – Data Breach Notification Statute
- 201 CMR 17.00 – Data Security Regulations
- M.G.L. c. 93I – Data Disposal Statute
- AGO responsible for enforcing data security statute and regulations

What is Personal Information?

- Different states have different definitions of PI under their notification statutes.
- First name and last name or first initial and last name of a resident in combination with one or more of the following:
  - SSN,
  - driver's license number or state-issued card id number; or
  - financial account, debit or credit card number.
M.G.L. c. 93H

- Data breach notification statute went into effect in October 2007
- Massachusetts 39th state to require consumer notification of data breaches.
- Currently 47 states have data breach notification statutes.

Notification of Data Breach

- When an entity experiences a data breach it must give notice of the breach to the AGO, OCABR, and affected consumers
- Notice required when:
  a) a breach of security; or
  b) personal information compromised
- Two distinct prongs
Notice to AGO and OCABR

• Notice to AG & OCABR must include three elements:
  • nature of the breach of security or the unauthorized access or use of personal information;
  • number of affected MA residents; and
  • steps the notifying entity is taking or plans to take, relating to the incident.

Notice to Consumers

• Notice to MA residents must include:
  • consumer’s right to obtain a police report;
  • how a consumer requests a security freeze;
  • information a consumer will need to provide to request a security freeze; and
  • disclosure of fees associated with placing, lifting, or removing a security freeze.
Federal and State Law

- Federal law notification requirements
- HIPAA and Gramm Leach Bliley Act
- M.G.L. c. 93H, Section 5
- If properly provide consumer notice under the federal statute, then have complied with the notification provisions of c. 93H.
- Notice to AGO still required.

Data Security Regulations

- 201 CMR 17.00 went into effect on March 1, 2010
- Requires all entities that own or license personal information about a Massachusetts resident to implement a WISP and computer system security requirements.
- OCABR implemented regulations and the AGO enforces the regulations.
201 CMR 17.00

• Owns or licenses means – “owns, 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.”
• Large hospitals and small practices

201 CMR 17.00

• Risk-based approach to information security in that the regulations direct businesses to establish a WISP that takes into account:
  • The size of the business;
  • The scope of the business;
  • The amount of resources of the business; and
  • The need for security of personal information.
Written Information Security Program

• The WISP shall include, among other things:
  • Assessment of reasonably foreseeable internal and external risks to the security of data containing personal information
  • Development of security policies for employees that take into account how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
  • Reasonable restrictions upon physical access to records containing personal information – keeping such records in locked facilities or storage areas.

©2012 Office of Massachusetts Attorney General Martha Coakley

Written Information Security Program

• Taking reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information consistent with the regulations and is applying to personal information such protective security measures.
• Require third party service providers by contract to maintain security measures for personal information.

©2012 Office of Massachusetts Attorney General Martha Coakley
Computer System Requirements

• To the extent technically feasible, these requirements include, among other elements:
  • control of user IDs and identifiers
  • 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
  • restrict access to records and files containing personal information to those who need such information to perform their job duties

©2012 Office of Massachusetts Attorney General Martha Coakley

Computer System Requirements

• Encryption of all transmitted records and files containing personal information that will travel across public networks (or wirelessly), and encryption of all data containing personal information to be transmitted wirelessly. Encrypt emails containing PI.
• Encryption of all personal information stored on laptops or other portable devices

©2012 Office of Massachusetts Attorney General Martha Coakley
Data Disposal Statute

- M.G.L. c. 93I – proper destruction of personal information
- Applies to both paper and electronic records
- Redacted, shredded, pulverized so nonreadable.

Enforcement

- M.G.L. c. 93H (Data Breach Notification Statute) charged OCABR with promulgating regulations and AGO with enforcing regulations
- Violation of 201 CMR 17.00 is a violation of M.G.L. c. 93A (Massachusetts Consumer Protection Statute)
- M.G.L. c. 93A allows up to a $5,000 penalty per violation
Enforcement

- AGO learns of data breaches through several different mechanisms including M.G.L. c. 93H notice, through whistleblower employees, through consumers, and through the media
- Data breach could trigger a letter from AGO, request for WISP, investigation (CID), and/or enforcement action

Enforcement

- Data security statute and regulations apply to all “persons” (a natural person, corporation, association, partnership, or other legal entity) who own or license personal information about a resident of the Commonwealth
- Large hospitals and small practices are both subject to the regulations
Enforcement

- When AGO learns of a breach it will examine several factors including:
  - Were affected consumers, AGO, and OCABR properly notified of the breach?
  - Did the owner of the data make false or misleading representations concerning the security of data?
  - Was the data stored or maintained in a manner so that it was not reasonably protected and therefore susceptible to a breach (unencrypted PI on laptops, unencrypted emails containing PI)?
  - Did the owner of the data have either no policies or inadequate policies in place with respect to protection of PI?
  - If reasonable policies were in place were they followed?

Enforcement

- Factors that may trigger request of WISP
- Size and nature of breach
- Electronic Information was not encrypted
- Multiple breaches in short time period
- Need for security and confidentiality of information
Enforcement

- Examination of WISP
- Is there a WISP in place?
- Contains all elements required under 201 CMR 17.03?
- Any elements of WISP clearly not being followed? If not, why?
- Who is the entity sharing PI with? What has that entity done to protect the PI it is sharing?

Enforcement Actions

- Consent Judgment with restaurant group – accepting payment card information without implementing basic security to protect information.
- Consent Judgment with hospital after failing to encrypt PI and PHI on lost backup data tapes
- Assurance of Discontinuance with local bank – had WISP in place but policies were not followed.
- Further examination of WISP and third-party vendor contracts
AGO Data Privacy Enforcement

State and Federal Law in Tandem

“…Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not be spoken of outside, I will keep secret, as considering all such things to be private…”

Excerpt from The Hippocratic Oath (National Library of Medicine and National Institute of Health)

©2012 Office of Massachusetts Attorney General Martha Coakley
Health Care Data Breaches reported to the AGO

HIPAA and the HITECH ACT

• *Health Information Technology for Economic and Clinical Health Act (HITECH Act)*

  • *Passed by Congress on Feb. 13, 2009*

  • *State Attorneys General authorized to bring civil lawsuits for HIPAA violations*
AGO Data Privacy Enforcement
A Nexus of Federal and State Law

Responsibility

• HIPAA – Covered Entity
• MA State data privacy Laws
  • “Every Person that 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.”
Share Wisely – Who? Who?

- 201 CMR 17.03(2)(f)(1)
  - “taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect [] personal information…”

Data Breach Reporting

- Required Self-Reporting
- AGO Complaints
- Patient reporting
"An ounce of Prevention,  
Is worth a pound of Cure."
- Benjamin Franklin
What personal data do you have?

- Protected Health Information (PHI)
  - Patient medical records
- Other Personal Information
  - Patient financial information; insurance information; payment information; SSNs; credit card numbers
  - Employee information

Where is your data?

- Inside the Office
  - Paper Files
  - Desktop and Laptop Computers
  - Network Servers
  - EMR
- Outside the Office
  - Portable Devices
  - Business Associates
- In the “Cloud”?
Who uses your data?

- Physicians
- Nurses, PAs, Assistants, Techs
- Office Staff

Who else has access?

- Other Health Care Providers
- Labs/Ancillaries
- Business Associates
  - Billing and coding providers
  - Data management providers
  - IT support
Top 5 Security Risks

1. Portable Devices
   • Wireless and Mobile devices
   • Laptops; flash drives; cell phones
   • Passwords vs. Encryption
   • Loss

Top 5 Security Risks

2. Theft
   • Office
   • Home Office
   • Cars
   • ID Theft
   • Hacking/Malware

©2012 Office of Massachusetts Attorney General Martha Coakley
Top 5 Security Risks

3. Transfer and Disposal (Part One)
   • Transfer
     • Medical records
     • Data

Top 5 Security Risks

3. Transfer and Disposal (Cont’d)
   • Data Destruction and Disposal
     • Paper
     • Electronic media – e.g., back-up tapes
Top 5 Security Risks

4. System Security
   • Security Settings
   • Employee Training

5. Business Associates
   • Third Party Service Providers
Contact Information

Office of Attorney General Martha Coakley
617-727-2200

Shannon Choy-Seymour
Shannon.choy-seymour@state.ma.us

Wendoly Ortiz Langlois
Wendoly.langlois@state.ma.us

Lois Johnson
Lois.johnson@state.ma.us

©2012 Office of Massachusetts Attorney General Martha Coakley

Thank you!