AHIP
America's Health
Insurance Plans

Implementing Effective Training Programs to Avoid Data Security Breaches

CMS/NIST Security Workshop: Implementation of the HIPAA Security Rule
Gaithersburg, Maryland

Presented By: Robert Talbot, Vice-President of Information Security for Coventry Health Care

January 16, 2008

About AHIP

AHIP
America's Health Insurance Plans

- AHIP is the national trade association representing nearly 1,300 health insurance plans providing coverage to more than 200 million Americans

- Our members offer a broad range of products in the commercial marketplace including health, long-term care, dental, vision, disability, and supplemental coverage

- Our members also have a strong track record of participation in Medicare, Medicaid, and FEHBP

- Our health insurance plan members comply with the HIPAA Privacy and Security requirements and have been proactive in the area of information security

About Coventry Health Care

America's Health Insurance Plans

- Coventry Health Care ("Coventry") is a diversified national managed healthcare company based in Bethesda, Maryland

- Coventry provides a full range of risk and fee-based managed care products and services to individuals, employer and government-funded groups, government agencies, insurance carriers and administrators, including commercial, individual consumer, Medicaid managed care, Medicare Advantage coverage, Medicare Private Fee for Service, Medicare Part D, and Federal Employees Health Benefits, and other specialty products

- In addition, Coventry has taken an industry leading approach for training staff about information security

HIPAA Overview

AHIP America's Health Insurance Plans

- The HIPAA Privacy and Security Rules provide an effective framework for protecting health data
  - Essential for Protecting Health Data
  - Consistent Set of Security Standards and Safeguards
  - Scalability and Flexibility Based on Unique Business Environments
  - Consumer Notice and Trust
- AHIP members comply with the HIPAA regulatory requirements as health insurance plans

Additional Requirements/ Considerations

AHIP America's Health Insurance Plans

- In addition to the HIPAA rules, most states have enacted data security requirements
  - Notice to consumers and/or consumer agencies
  - Remedial actions in the event of a data breach

- From a practical standpoint, all public and private entities should anticipate and prepare to handle security risks and threats

- Public expectations for public and private entities to protect confidential data
  - Employer/customer expectations
  - Individual consumer demands
  - Competitive advantages

Main Issue

- Focus of the Presentation is the use of training programs to prevent data security breaches

- While technical intrusions (e.g., hackers) can create security incidents and cause data breaches, human error can be a cause or contributing factor
  - Mistakes
  - Error in following security policies
  - Not knowing what a “Security Incident” is
  - Not understanding to whom to report security incidents

HIPAA Framework: Preventing and Responding to Data Breaches

- The HIPAA Security Rule:
  - – Defines a “security incident” (45 C.F.R. §164.304)
  - – Sets detailed requirements for administrative, physical, and technical safeguards to protect health data (45 C.F.R. §§164.304 - 318)
  - – Lists rules for conducting risk analysis and risk management activities (45 C.F.R. §164.308)
  - – Requires security awareness training (45 C.F.R. §164.308(a)(5))
  - – Requires entities to have security incident procedures, including identification, response, mitigation and documentation (45 C.F.R. §164.308(a)(6))

Effective Training Programs

AHIP America's Health Insurance Plans

- Should convey:
  - – the content of security policies;
  - – where to access;
  - – who receives reports of security incidents;
  - – who investigates;
  - – examples of how the company monitors and detects intrusions;
  - – examples of data breaches and remedial measures, including the kinds of behaviors that can result in or prevent a data breach;
  - – specifics about how to document incidents and breaches; and
  - – information about the frequency of updates.

Preventing Security Breaches

AHIP
America's Health Insurance Plans

- Establishing and Communicating Security Policies and Procedures
- Training
- Ongoing monitoring
- Updating Policies and Procedures
- Re-Training
- Being Current with Legal and Technical Requirements

Current and Future Environments

- Existing and New Business Operations
  - Personal Health Records, Electronic Health Records
- National, Electronic Information Exchange
- Movement of Data, Including Mobile Devices
- Collection of Health Data by Entities not Covered by HIPAA
- Emerging Trends
  - Hacking
  - Other Criminal Activity
- New Security Standards
- Industry Best Practices

AHIP Supports

America's Health Insurance Plans

- HIPAA as an effective framework to protect privacy and security of individually-identifiable health data
- Requiring business entities and government agencies to establish security programs to protect consumer data, without creating duplicate or conflicting requirements
- A national, federal standard for notifying consumers if their information is part of a data breach
- Voluntary practices that promote collaboration and better understanding of security practices

Recommendations

- CMS/NIST should continue to develop guidance about regulatory and security requirements

- CMS/NIST should continue to work with the private sector and governmental agencies to facilitate understanding of consistent security policies and applications

- NIST should continue to issue guidance focused on technical requirements and infrastructures

Thank You

- Thank you for the opportunity to testify. I would be happy to take any questions.

Robert Talbot
Vice President, Information Technology
Coventry Health Care
retalbot@cvty.com
480-445-4848