



Information Security for Health Plans

HCCA Managed Care Compliance Conference

February 23, 2009

Jeannette Frey

Privacy Officer

Fallon Community Health Plan, Inc.

Worcester, MA

Jeannette.frey@fchp.org

978-368-9382

Fallon Community Health Plan

- Our mission: Making our communities healthy
- Founded in 1977
- Massachusetts based, non profit
- Membership: 217,563
- Products: Commercial and government programs
 - Commercial HMO, PPO, and POS plans fully-insured and self-insured
 - Fallon Senior Plan™ (Medicare Advantage)
 - Summit ElderCare® (Program for All-Inclusive Care for the Elderly)
 - FCHP MassHealth (Medicaid)



Overview

- Integrating security with privacy and compliance
- Health plan security requirements
- Recent enforcement activities
- Risk areas and challenges



Challenges Integrating Security with Privacy and Compliance Programs



Privacy vs. Security

- What's the difference?



Why Integrate?

- Privacy and compliance programs are historically outward facing and touch all areas of the company
- Privacy and compliance programs have extensive experience writing policies and procedures and training the workforce
- Privacy and compliance have experience working with business, can speak the language



Successes

- Privacy and Security Committee
 - Provides oversight, direction to the privacy and security programs
 - Cross section of the company (e.g. Operations, IT, Compliance)
 - Co-chaired by Privacy Officer and Security Officer
 - Monthly agendas developed together
- Weekly meetings with Privacy Officer and Security Officer
- Daily phone conversations between Privacy Officer and Security Officer!



Health Plan Security Requirements

HIPAA Security Regulations
Payment Card Industry (PCI) Standards
State Laws
Contractual Requirements (CMS and Employers)



Information Health Plans Maintain

- Medical information/protected health information (PHI)
- Identifying information for members, employees, and providers
 - Social Security Numbers
 - Dates of birth
- Financial information for members, employees, and providers
 - Credit card numbers
 - Tax ID numbers
 - Checking account and banking information



HIPAA Security Regulations

- Who must comply?
 - Health plans (includes both insurers and group health plans, e.g. employee welfare benefit plans)
- What information do the regulations apply to?
 - Electronic protected health information (ePHI) which is individually identifiable health information of
 - Members
 - Employees who are members of the group health plan
- What information do the regulations not apply to?
 - Information about providers
 - Information about employees



HIPAA Security Regulations

- Requires covered entities to ensure the confidentiality, integrity, and availability of ePHI
- Implement physical, technical, and administrative safeguards to protect PHI
 - Physical: e.g. access controls, device and media controls
 - Administrative: e.g. security management process, security officer, policies and procedures, training
 - Technical: e.g. access controls, audit controls, integrity, transmission security
- Reasonableness standard; scalable and flexible



HIPAA Security Regulations

- HIPAA Security Regulations are enforced by CMS
- CMS has issued guidance on interpretation and meaning of the HIPAA Security Regulations
 - *HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information* published December 28, 2006
 - *HIPAA Security Educational Paper Series*



Payment Card Industry (PCI) Standards

- Purpose of the PCI standards is to prevent credit card fraud
- Who must comply?
 - Merchants and their vendors who store, process, or transmit credit card data
 - Must comply via contract with the bank that processes payments
- What information do the standards protect?
 - Cardholder data (credit card information, security code, etc)
- Proof of compliance depends on the number of yearly transactions performed (e.g. self assessment v. certified auditor)



Payment Card Industry (PCI) Standards

- Standards require merchants and vendors to:
 - Have a secure network (e.g. firewalls and strong passwords)
 - Protect cardholder data (e.g. encrypt stored data and data transmitted over public networks)
 - Have a vulnerability management program (e.g. antivirus)
 - Have strong access controls (e.g. unique user IDs, restricting physical access)
 - Monitor and test networks (e.g. track all access, test security)
 - Have a security policy



State Laws – Massachusetts General Law 93H and 201 CMR 17.00

- Massachusetts law requiring notice to individuals in the event of a security breach and requires adoption of regulations designed to safeguard personal information.
- Who must comply?
 - Any person (e.g. person, corporation, association) that owns or licenses personal information about a resident of Massachusetts
- What information do the regulations apply to?
 - Personal information in paper or electronic form
 - First name and last name (or first initial and last name) and at least one of the following: Social security number, drivers license number, or financial account number, or credit, or debit card number
- This definition will apply to employee information, provider information and all member information in paper form.



State Laws – Massachusetts General Law 93H and 201 CMR 17.00

The security requirements in this law and regulation include:

- Ongoing risk assessments, development of policies and procedures, training of staff, designation of security officer
- Implementing secure authentication protocols
- Implementing secure access control measures
- Encryption of all records transmitted over a public network and transmitted over a wireless network
- Monitoring for unauthorized use of or access to personal information
- Encryption of personal information stored on laptops or other portable devices
- Contractually require service providers to protect data and obtain a written certification from service providers that it has a written, comprehensive information security program in place that is in compliance these regulations.



Contractual Requirements – Employers Fully insured and Self insured

- Employer groups (both fully insured and self insured) are attempting to contractually require plans to implement privacy and security protections sometimes over and above what HIPAA Security requires
 - Notification if a breach occurs
 - Notification prior to disclosing PHI
 - Specific security protections, e.g. encrypting laptops, password requirements



Contractual Requirements – CMS Medicare Advantage and Part D Plans

- Entities contracting with CMS are contractually required to comply with all State and Federal laws related to confidentiality and non-disclosure
- CMS has issued a number of directives related to security:
 - 2009 Call Letter requires specific security safeguards be implemented
 - CMS CIO Directive dated August 21, 2007, requires Medicare contractors including Medicare Advantage Contractors and Prescription Drug Plans to comply with its *Information Security Handling Procedure and Breach Analysis/Notification Procedure*
 - CMS Memorandum from Abby Block dated December 16, 2008 outlining security requirements and process for notifying CMS of security breaches
- These directives and memos apply to PII
 - Personally Identifiable Information
 - Any information about an individual which can be used to distinguish or trace an individual's identity



Contractual Requirements – CMS Medicare Advantage and Part D Plans

Security requirements outlined in these directives/memos:

- Encrypting PII on all portable devices
- Ensuring PII is not saved on public or private computers when accessing e-mail through the Internet
- Ensure electronic systems are properly programmed for beneficiary mailings in order to prevent documents containing PII from being sent to the wrong beneficiaries
- Perform risk assessment and “quickly” remedy weaknesses or gaps
- Train staff
- Document compliance with HIPAA Privacy and Security rules
- Report security incidents according to CMS’s process



Other

- Gramm Leach Bliley
- NAIC Model Audit Rule
- FTC
- Red Flag Rules
- Industry security standards
 - ISO 27000
 - COBIT



Summary

- Be sure to check the scope of the requirement
- Requirements might be similar to HIPAA but the scope is different
- Scope might be the same as HIPAA but the requirements are different
- Remember your employees' information
- Remember your providers' information
- Don't forget about paper!!



Enforcement Activity



CMS Enforcement of HIPAA Security

- HIPAA Security Regulations are enforced by CMS (Office of E-Health Standards and Services)
- 392 complaints to CMS as of December 2008
 - 305 resolved
 - 87 still open
- Categories of complaints (Michael Phillips, Information Systems Security Officer OESS/CMS)
 - 90% of the allegations were from someone inside the organization alleging someone is using information inappropriately (e.g. family member or employee)
 - Less than 10% are complaints involving loss or theft of devices but accounts for most of data/information exposed
 - Insufficient access controls for systems containing ePHI (e.g. shared passwords, lack of encryption)



CMS Enforcement of HIPAA Security

Compliance Reviews

- CMS has authority to conduct compliance reviews as they deem necessary
 - Will provide description of the complaint
 - Onsite review will look at policies and procedures and systems
 - Focus on remote access policies and procedures
 - See the *"Sample – Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews"* Issued by OESS in CMS
- CMS has authority to impose civil monetary penalties
- CMS contracted with Price Waterhouse Coopers to perform ten compliance reviews during 2008
 - Focus was on entities that a complaint had previously been filed against
 - Findings showed lack of encryption for portable devices and media and lack of verification of role based access privileges



CMS Enforcement of HIPAA Security

OIG Security Audit

- First OIG audit; Piedmont Hospital
- March 2007-June 2007
- Purpose was to assess CMS enforcement of Security Rule
- Other audits have also occurred

Resolution Agreement

- First Resolution Agreement; Providence Health Systems
- As a result of four stolen back-up tapes that were not encrypted and 4 stolen laptops that were not encrypted which compromised the PHI of almost 400,000 patients
- 31 complaints to OCR and CMS
- Providence did not follow its own policies and procedures
- Resolution payment of \$100,000 and under corrective action plan for 3 years
- Not a Civil Monetary Penalty



State Enforcement

- Delaware Insurance Commission fines Blue Cross \$150,000 for privacy violations
- Mailing error that caused 3,800 explanation of benefits to be mailed to the incorrect member
- Insurance Commission argued the mailing error violated two provisions of state law
 - Prohibition on disclosure of nonpublic personal, financial information about a consumer, and
 - Requirement that insurers have systems in place to safeguard customer information



Risk Areas and Challenges



Point Solutions

Challenges/Risks

- Stand-alone systems that address specific business needs are disparate and decentralized
- Creates a challenge with maintaining consistent security policy and enforcement across each solution
- Access databases

Solutions

- Centralize ownership of system within IT, not the business area
- Manage access rights and termination through IT



Portable Devices and Laptops

Risks/Challenges

- Large amounts of PHI and confidential information can be stored on portable devices (e.g. CDs, flash drives) and laptops
- Easily lost
- Target for theft

Solutions

- ENCRYPT!!!!
- Prohibit the storage of PHI or confidential information on portable devices and laptops unless they are encrypted
- Use Lost Data Destruction software
- Consider solutions that monitor the movement of PHI in transit (will tell you when someone saves PHI to a disc or flash drive)



Business Associates and Vendors

Challenges/Risks

- Companies look to lower costs by outsourcing.
- Disclosure of PHI and other sensitive information is more common
- Difficult to monitor and oversee business associates
- Disclosures to potential vendors for return on investment analysis

Solutions

- Centralize the vendor selection and contracting process
- Perform security assessments as part of due diligence
- Protect yourself contractually. Use standard business associate contracts that contain the required provisions. Consider adding additional provisions, e.g. insurance, indemnification, certificate of destruction.
- Secure transmission of PHI
- Ongoing monitoring/auditing of business associates



Employer Contracting

Risks/Challenges

- Employer has security requirements that you can't or don't comply with
- Seemingly competing goals for Sales v. Security

Solutions

- Get involved in employer contracting
 - Drafting and reviewing RFP responses
 - Responding to questionnaires
 - Review contract provisions and business associate agreements
- Develop strong relationship with Sales department and understand the business perspective
- Be ready to explain why you can't agree to a particular provision



Others

- System access controls
 - Role based access
 - Restricting access while being flexible to meet business needs
- Remote access and telecommuting
- Collection of and security of social security numbers
- Training!!!



Conclusion

- Many requirements that must be met, not just HIPAA
- Information security is an ongoing, never-ending process
- Compliance is the right thing to do for your company, your customers, and your members



Questions

