



Health Plan Information Security: Preventing and Responding to Data Breaches

HCCA Managed Care Compliance Conference
February 23, 2009

Anne Doyle
EVP, Chief Compliance Officer
Fallon Community Health Plan, Inc.
Worcester, MA
Anne.Doyle@fchp.org
978-368-9433

I wish to acknowledge that a significant portion of this presentation was prepared by and is used with permission of Linda A. Tomaselli, Esq. while a member of Epstein Becker & Green, P.C.

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, POS and PPO 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

Preventing and Responding to Data Breaches

- Extent of the challenge
- Best practices to secure data and prevent a breach
- Responding and doing the right thing
- Notification requirements: who, what, when?



3

What is your risk?

- **What?**
 - Protected Health Information (PHI), Personally Identifiable Information (PII)
 - Demographic information (including Social Security Numbers)
 - Health information
 - Credit Card numbers
 - Tax Identification numbers (for providers)
- **Where?**
 - Paper documents
 - Electronic - data warehouse, business applications/systems, servers, laptops, hard drives, network drives, email, back-up tapes, wireless devices, voicemail services, electronic medical record and MORE
- **How?**
 - “at rest”
 - “in-transit”



4

Extent of the Challenge

- Financial fraud
- Medical Fraud
- Third-party data breaches increasing in number and in cost vs. internal breaches
- Per-record cost of data breach \$197 in 2007 (est.)
 - Estimated cost per record for *third-party data breach* even higher
 - **Greatest component cost: lost business**

Source: Ponemon Institute LLC, 2007 Annual Study: U.S. Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions (Nov. 2007).



5

Recent Data Breaches

- **UCLA Medical Center - 2008**
 - Former employee indicted after selling medical record information of celebrities including Farrah Fawcett, Britney Spears and Maria Shriver. Reports of breaches involving at least 61 patients. Other UCLA employees resigned or were fired, and physicians suspended, for accessing records of Spears.
- **Horizon BCBS of New Jersey - 2008**
 - 300,000 personal information, including SSNs, was stolen.
 - No medical data involved
 - How: Employee laptop computer stolen.
- **HHS and Providence Health & Services- July 2008**
 - **Resolution Agreement including Corrective Action Plan to Protect Health Information:** \$100,000 fine and a Corrective Action Plan. CMS reserved right to impose further (civil monetary) penalties.
 - Enforcement stems from incidents involving 386,000 patients at Providence facilities where unencrypted backup tapes, optical disks, and laptops, all containing health information, were removed from the premises and left unattended.



6

CMS resolution in the Providence Breach confirms the challenge

“This resolution confirms that effective compliance means more than just having written policies and procedures. ***To protect the privacy and security of patient information, covered entities need to continuously monitor the details of their execution, and ensure that these efforts include effective privacy and security staffing, employee training and physical and technical features.***”
CMS (emphasis added)



7

**How does your
organization prevent a
breach?**



8

Best Practices for Avoiding Breaches Privacy and Security Culture

Strong **Culture** of Security and Privacy

- Accessible and pervasive privacy program
- Visible Corporate Compliance Program
- Behaviorally-based training and communications
- Encouragement to speak up
- Enforcement of privacy/security breaches
- Strong Oversight: Compliance Committee, Privacy and Security Steering Committee, Board Audit and Compliance Committee
- Active involvement by senior management and the board



9

Best Practices for Avoiding Breaches Ongoing Risk Mitigation

Enterprise Risk Management Program

- identify privacy and security risks
 - Laptops and portable devices*
 - Portable Media (e.g. CDs, back-up tapes)
 - Vendors
 - Employees
- assign accountability
- address gaps/mitigate risks
- assess periodically and as warranted

*Laptops and portable devices accounted for 49% of total 2007 data breaches. Ponemon Institute LLC, 2007 Annual Study: U.S. Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions, 11 (Nov. 2007)



10

Best Practices for Avoiding Breaches Ongoing Risk Mitigation



Source: Adapted from Terasen Inc. Conference Board 2005 *From Risk Management to Risk Strategy*

Best Practices for Avoiding Breaches The Nuts and Bolts

- Develop and keep up-to-date Incident Response Policy (including guidelines for communicating with external parties)
- Develop and keep up-to-date privacy and security policies and procedures including procedures around proper destruction/disposal of PHI/PII
- Inventory and understand nature of data maintained by entity; minimize PHI/PII
- Implement appropriate administrative, physical and technical safeguards
- Train and re-train employees
- Monitor and audit security
- Perform due diligence when outsourcing and have strong contract provisions
- Be prepared!

How will your organization respond to a breach?



13

Investigating and Responding to Suspected Breaches

- Before a breach occurs, have a plan
- Goal is to avoid a breach, if that fails, follow your plan
- Respond immediately and appropriately
- Prepare to spend money and time to address properly
- The investigation and response will take longer than you think
- Even small breaches need thorough investigation and response



14

Responding to Suspected Breaches Step-by-Step

1. Assemble an in-house multidisciplinary response team (management, board, IT, compliance, legal, communications, privacy officer, security officer, others)
2. Perform investigation (including forensic assessment)
3. Contain the risk and mitigate
4. Secure systems and return to pre-breach status
5. Identify potential stakeholders
6. Develop and implement response plan
7. Develop and implement internal and external communications strategy (including notice to members, stakeholders, regulatory agencies)
8. Conduct final assessment and lessons learned



15

Perform Investigation

- Get all the information
 - How do you know your data are missing?
 - What information do you have to support the breach and who is the source?
 - Is this a limited or extensive breach?
 - Who was involved—employee(s), vendor, vendor's subcontractor?
 - Exactly what members and information were effected?
 - Exactly what happened? How was the information breached?
 - Was it accidental or was it caused by theft?
 - Were appropriate policies, access controls, security, contracts, Business Associate Agreements (as applicable) in place?
- The answers to these questions will help dictate how you respond to the breach



16

Identify potential stakeholders

- Internal team
- Senior Management and Board of Directors
- Members and their families
- Regulators (CMS, State Attorney General, Division of Insurance, other state agencies)
- Press/Media
- Vendor(s) and their subcontractor(s) (if applicable)
- Vendor's insurance company (if applicable)
- Plan's insurance company (if applicable)
- Outside counsel
- Employees
- Other



17

Develop and Implement Response Plan

Respond according to the size and impact of the breach

- Educate/re-educate employees
- Create/update/distribute policies and procedures
- Contact the member(s) – phone/mail
- Contract with credit monitoring agency (in advance)
- Prepare customer service representatives (hire additional if needed to handle member influx of calls)
- Determine notification requirements and notify
- Track the chronology of events – document
- Communicate internally and externally
- Address HR issues, if any
- Address vendor issues, if any
- Hold a lessons learned session after you have handled the breach



18

Develop and Implement Communication Strategy

- Tone Matters
- “What would we do for our mother or grandmother?”
- Saying you are sorry...What you say and how you say it matters
 - What does your Attorney advise?
 - What does your company culture advise?
- Prior relationships with your stakeholders matter
 - Your stakeholders’ responses will be influenced by how you have related to them in the past.



19

Who does your organization need to notify about the breach? What must be reported and when?



20

Relevant Authorities/Exposure

- ✓ HIPAA – duty to mitigate
- ✓ Other federal law and agency oversight (e.g., CMS; FTC). CMS: duty to report; potential contract violations, fines, penalties
- ✓ State law and regulation – including security breach and notification statutes
- ✓ Contractual obligations with potential reporting (e.g., large employer groups)
- ✓ Private rights of action

Trend toward greater government enforcement



21

HIPAA

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - Requires covered entities to protect against reasonably anticipated threats to the security or integrity of electronic PHI and to protect against impermissible use or disclosures of such information.
 - Requires ongoing security risk analysis to detect and assess threats and fix vulnerabilities in information systems
 - Requires actions to mitigate: “A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of [PHI] in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.” §164.530(f)



22

CMS Guidance: Remote Access and Use; Audits

- CMS HIPAA Security Guidance (Dec. 2006)
 - Addresses remote access and use
 - Develop accurate and thorough risk assessment, and develop risk mitigation strategy linking directly back to assessment
 - Annually assess entity implementation viz. remote use and access guidance
- CMS Audit Guidelines (“Sample - Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews”)



23

CMS Directives: Notification

- CMS holds entities to a contractual obligation to abide by all Federal and State laws regarding confidentiality and non-disclosure.
- December 2008 Letter from Abby Block, Director, Center for Beneficiary Choices to Medicare Advantage Organizations and Prescription Drug Plans
 - “If there are any security incidents, **including those of a downstream entity**, it is the responsibility of the plan to report this information to CMS...”
 - “For security incident involving PII, organizations should report **within one hour of discovery/detection:**” (provides additional clarification depending on incident)
 - “Your CMS Account Manager will be your point of contact in communicating next steps...”



24

CMS Directives (continued)

- CMS Information Security Incident Handling and Breach Analysis/Notification Procedure (Version 2.0 August 16, 2007)
 - Appears initially to govern internal government breaches, but provides that “the procedure is incorporated by reference into CMS contracts and agreements” (page ii)
 - **Report within one hour of discovery/detection** (p.2) Security and Privacy Standards for Part D Sponsors—mitigating risk of ID theft in the event of a data loss or breach (p.77)
- Sponsors should notify CMS **immediately** upon discovery of any security breach compromising beneficiary PII (Chapter 5, Section 80)
www.cms.hhs.gov/PrescriptionDrugCovContra/Downloads/CallLetter.pdf
- June 2006 Letter from Abby Block, Director, Center for Beneficiary Choices to Medicare Advantage Organizations and Prescription Drug Plans
 - “[P]lans should notify CMS **immediately** upon discovery of any security breach compromising beneficiary personally identifiable information



25

HHS Enforcement

- Privacy and Security Rules are enforced by HHS’ Office for Civil Rights (OCR) and CMS
 - OCR and CMS have successfully resolved over 6,700 Privacy and Security Rule cases by requiring the entities to make systematic changes to their health information privacy and security practices.



26

STATE DATA BREACH



27

State Data Breach Activity

- California 1st state to enact data breach law, effective 2003; since extended to medical data
- Within 5 years, at least 43 additional states, the District of Columbia and Puerto Rico have adopted data breach laws.
 - Only Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota do not have statutes specifically addressing data security breaches.

Source: <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm> (last updated 9/16/08)



28

State Law Differences

- Key differences among state notification laws can significantly impact response strategies.
 - Reporting
 - Reporting to AG and/or other agencies and consumers
 - How to report, what to report and when to report it
 - Definitions can vary in significant respects
 - Personal information
 - Medical information
 - Financial information
 - Breach



29

Example: Mass. Security Breach Law

- October 31, 2007, Any person, entity, or government agency that owns or licenses (or maintains or stores) data including “personal information” must notify an affected Massachusetts resident “as soon as practicable and without unreasonable delay” if it knows or has reason to know:
 - of a breach of security, or
 - that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.
- Massachusetts General Laws ch. 93H (“Security Breaches”) also requires notification to the Attorney General and to the Director of Consumer Affairs and Business Regulation.
- The entity must also provide notice to credit reporting agencies and other state agencies if/as directed by the Director of Consumer Affairs.

Mass. Gen. Laws ch. 93H, § 3.



30

Appendix- Helpful Resources

1. CMS (Abby L. Block) Letter, December 16, 2008 Privacy and Security Reminders and Clarification of Reporting Breaches
2. CMS (Abby L. Block) Letter, June 9, 2006 to Contractors re: Privacy and Security
3. CMS Information Security Incident Handling and Breach Analysis/Notification Procedure (Version 2.0, August 16, 2007) (Includes Appendix B: Incident Response Template)
4. CMS Sample - Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews (Audit Checklist)
5. HHS HIPAA Security Guidance (12/28/2006)
6. Massachusetts Attorney General's Office Sample Data Breach Notification Letters:
 - * to the Attorney General
 - * to affected Massachusetts Residents



31

Questions



32