Seven Strategies for a Successful Patient Privacy Monitoring & Compliance Program

FairWarning® Executive Webinar Series
November 6, 2012
Agenda

Seven Strategies for a Successful Patient Privacy Monitoring & Compliance Program

- What is Required?
- What the Data Says
- Risks and Issues
- The Solutions: Seven Strategies
- The FairWarning® Patient Privacy Monitoring Center
- Q&A session
Today’s Panel

Donnetta Horseman
AVP and Corporate Responsibility Officer
CaroMont Health
Donnetta.Horseman@caromonthealth.org

Kurt J. Long
FairWarning® Founder and CEO
Kurt@FairWarning.com

Chuck Burbank
FairWarning® Director of Privacy Monitoring & Remediation Services
Chuck@FairWarning.com
Seven Strategies for a Successful Patient Privacy Monitoring & Compliance Program
Donnetta Horseman, AVP & Corporate Responsibility Officer
CaroMont Health, Gastonia NC
About CaroMont Health

We are a nationally recognized leader and valued partner in promoting individual health and vibrant communities

- 3,800 employees
- 452 medical staff
- 268 volunteers
- Gaston Memorial Hospital, 435 beds
- CaroMont Medical Group, a network of 45 primary & specialty physician offices in 5 counties & 2 states
- Courtland Terrace, 96 bed skilled nursing facility
- Gaston Hospice
About Me

• 26 years in Health Care
• 6+ years in IT and Telecom
• 7+ years in Compliance and Privacy
• Master’s Degree in Management
• Certified in Health Care Compliance
• Certified Information Privacy Professional/US
• Certified Compliance Executive
What is Required?

Health Insurance Portability and Accountability Act – HIPAA

§164.308(a)(1)(ii)(D): Security Management Process - Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Audit Procedures

Inquire of management as to whether formal or informal policy and procedures exist to review information system activities; such as audit logs, access reports, and security incident tracking reports. Obtain and review formal or informal policy and procedures and evaluate the content in relation to specified performance criteria to determine if an appropriate review process is in place of information system activities. Obtain evidence for a sample of instances showing implementation of covered entity review practices. Determine if the covered entity policy and procedures have been approved and updated on a periodic basis.
What is Required?

- HITECH Accounting for Disclosures Rule
- Effective date – January 1, 2014
  - If we use an electronic health record, we must be able to provide accountings of disclosure for treatment, payment and operations
  - All electronic health record systems must be able to track and report out in a format that can be delivered to patients any disclosures made for treatment, payment and operations purposes beginning with disclosures that occur after January 1, 2014.
• Majority of breaches committed by employees
• 35% snooping into medical records of fellow employees
• 27% accessing records of friends and relatives

Source: Veriphyr’s 2011 Survey of Patient Data Breaches
Where We Started

2010

• Many systems and applications
• IT Guru created Access Database
• Uploaded audit logs from system, ran reports
• Extremely time consuming
• Required specific expertise
• Had to match up data from multiple systems
Risks and Issues

- No way to conduct proactive audits
- Staff knew that “no one was watching”
- High incidence of staff snooping and looking at their own records
- Very long time to complete investigations
- Many systems not getting audited at all, some didn’t even have audit logs turned on
The Solution: 7 Strategies

- Policies
- Education
- Prevention
- Breach Notification
- Incident Investigation
- Detection
- Audits
Policies

• Role and Purpose Based Access to PHI
• External Data Release
• User Confidentiality Agreement
• Mobile Device Security
• Email and Internet Use
• Disciplinary Action
Education

- Computer-Based Modules
- In person training
- Newsletters
- Posters
- Make sure staff know your policy on snooping and looking at their own records
- HIPAA Privacy & Security Basics
Prevention

- VIP Record Lockdown
- Education and Awareness
- Audits
- Disciplinary Action
Audits

• Inventory systems/applications
• Turn on audit logs
• Generic user ID’s
Detection

- Hotline reports
- Policy implementation
- Department spot checks
Incident Investigation

• Incident Investigation and Response Plan
• Who will do what?
• What kind of information needs to be gathered?
• Was there a breach?
• Does it require notification?
  – NCHICA Breach Risk Assessment Tool

http://www.nchica.org/hipaaresources/Documents.htm
Breach Notification

• Develop template notification letters
• Plan in advance
• Credit Monitoring
• HHS Notification
• Media Notification
• Consider insurance
My 3 Wishes

• A tool to aggregate audit logs into one place
• Marry up user ID with HR data
• Show all systems accessed and exactly what functions were completed
  – Print
  – View
  – Change
• Privacy Breach Detection systematically identifies users who are engaging in patient access patterns that are indicative of snooping, identity theft or other risky behaviors.

• Privacy Breach Detection is performed for all crucial EHRs and applications, which provide access to electronic Protected Health Information (ePHI).

• Privacy Breach Detection then filters out known false positives, and brings any remaining potential incidents to the attention of appropriate privacy personnel.
• FairWarning® allows for the creation of enforced policies that map directly to specific compliance requirements.

• When a policy violation is identified, an alert is sent, providing peace of mind that non-compliant accesses will be identified on a proactive basis.

• FairWarning® addresses auditing and monitoring requirements of a variety of regulations, eliminating the headache of conducting these activities manually and allowing Compliance staff to focus on other priorities.
FairWarning® Patient Privacy Portal provides a comprehensive dashboard for compliance tasks including:

• Enforcing compliance policies
• Identifying the biggest potential areas of non-compliance
• Tracking issue resolution for compliance effectiveness
• Providing enterprise-level reporting for executive and board audiences
Tool Implementation

- Identify applications/systems to audit
  - Technical challenges, timeframes, learning curve of audit log language, IT involvement, etc.
- Define who would manage, conduct audits
- Determine what alerts to set up
- Run test audits
- Review alerts and reports
Implementation (cont.)

• Investigation and Response
• Disciplinary Actions
• Breach Notification
• Staff Education
Privacy Violations
Next Steps

- Continue to add audit sources
- Implement family member snooping alerts
- Continue education
- Review and update policies on a regular basis
- Track and trend
For more information:

Donnetta Horseman
AVP & Corporate Responsibility Officer
CaroMont Health

donnetta.horseman@caromonthealth.org
704-834-4846
Introducing The Patient Privacy Monitoring Center
PrivacyServices@FairWarning.com
"Patient Privacy Monitoring" found to be #1 deficiency in **first 20 HIPAA audits** according to Office for Civil Rights

More than **100,000 care providers** have adopted EHRs and realize payments under **Meaningful Use**

**27% of US patients** withhold medical information due to privacy concerns

**85% of patients** indicate that a care provider’s reputation for protecting privacy influences their choice to seek care from that provider

An estimated average of **2 million Americans** are victims of medical identity theft yearly, with an estimated total cost of **$41 billion**

Sources: New London Consulting US Survey; Ponemon Study; HHS.gov; OCR NIST Presentation on Security Compliance
OCR established a comprehensive audit protocol containing criteria to be assessed during audits. FairWarning® directly maps to patient privacy criteria. [Click here](#) to see how customers are aligning FairWarning® to regulatory requirements.

<table>
<thead>
<tr>
<th>Section</th>
<th>Established Performance Criteria</th>
<th>Key Activity</th>
<th>Audit Procedures</th>
<th>Implementation Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.312</td>
<td>§164.312(b) Audit Controls - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</td>
<td>Select the Tools that Will be Deployed for Auditing and System Activity Reviews</td>
<td>Inquire of management as to whether systems and applications have been evaluated to determine whether upgrades are necessary to implement audit capabilities. Obtain and review documentation of tools or applications that management has identified to</td>
<td>Required</td>
</tr>
<tr>
<td>§164.312</td>
<td>§164.312(b) Audit Controls - Implement</td>
<td>Develop and Deploy the</td>
<td>Inquire of management as to whether a formal</td>
<td>Required</td>
</tr>
</tbody>
</table>
Reality for Care Providers

• Compliance, privacy, and security projects are competing for same resources
• Compliance, privacy, and security experts are in high demand and “stretched thin”
• Poorly implemented privacy monitoring project could bring greater compliance and risk exposure
• HHS OCR audits continuing and bring risk of non-compliance
Introducing the Patient Privacy Monitoring Center

- FairWarning® expert personnel operate on-going patient privacy monitoring in cooperation with care provider
  - Conducts patient investigations
  - Create analytics and filters for best-of-class privacy monitoring
  - Monitor analytics for privacy breaches
  - Prepare governance and audit reports

- Designed to achieve a “Fully Defensible” position for care provider with regard to patient privacy auditing

- Optional service for FairWarning® customers

- Utilizes FairWarning® product technology
Leverages Best-of-Class Platform
FairWarning® 3.1

Compatible with Every Major EHR and Over 185 Applications Used in Healthcare

User and Patient Access Reports

Privacy Breach Detection Analytics and Alerts

Governance and Compliance Effectiveness

Investigations and Legal Defense

Collaborative Patient Privacy Monitoring
Leverage best practices and expertise from customers representing over 1,000 hospitals in 45 states

1. Benchmark across our customers, approximately **5 out of 1,000 admissions results in an electronic privacy breach.**

2. **Employee as patient snooping** is a universal privacy concern that has quality of life and economic impact.

3. Identity theft in urban settings using ePHI for various forms of financial and medical fraud.

4. VIP and neighbor snooping is a concern for care providers of all sizes and types that causes reputational damage and loss of trust.

5. Privacy breaches are often symptoms of fraud – misuse of access to ePHI is directly linked to medical fraud.

Additional Reference:
Monitoring Center Highlights

Leverage our team of privacy experts to bridge gaps in resources or expertise to implement a world class patient privacy program.

Program highlights:

– Communication and education plans
– Standardized workflows
– Proven validation/remediation processes
– Review of applicable policies with suggested additions or updates
– Guidance on documentation of decisions around the deployment of FairWarning® Patient Privacy Monitoring technology
– Implementation and monitoring of a series of proven automated enforced policies
– Review/investigation of triggered enforced policies
– Assistance access reviews triggered by patient privacy complaints
Customer Responsibilities

• Carry out the communication plan and staff education regarding the program

• Identify appropriate customer management personal for incorporation into standardized workflows and validation processes

• Perform a review of applicable policies

• Ensure timely management response to validation request regarding access

• Provide IT support as needed for additional data elements and ensure system backups
Benefits Summary
Patient Privacy Monitoring Center

- Expert services at a fraction of in-house expense
- Achieve a fully defensible position and a culture of patient privacy
- Leverage expert staff
  - Regulatory compliance and external auditor experience
  - Investigations
  - Sensitive situations
- Leverage findings from customers representing over 1,000 hospitals
- Leverage best-of-class technology
Contact Us

Donnetta Horseman
AVP and Corporate Responsibility Officer
CaroMont Health
Donnetta.Horseman@caromonthealth.org

Kurt J. Long
FairWarning® Founder and CEO
Kurt@FairWarning.com

Chuck Burbank
FairWarning® Director of Privacy Monitoring & Remediation Services
Chuck@FairWarning.com