Joining Forces for Patient Privacy: Compliance and Security Working Together

FairWarning® Executive Webinar Series
December 11, 2012
Joining Forces for Patient Privacy: 
Compliance and Security Working Together

• Roles that people, processes and technology play in successful patient privacy and regulatory compliance
• How Compliance teams can help Security teams to determine and understand the technical specifications during a Patient Privacy project’s discovery, planning and implementation phases
• Day-to-day cross-departmental operational support needed to support a successful patient privacy monitoring program
• The Business Case for Privacy Monitoring
• FairWarning® Managed Services
• Questions
Today’s Panel

John Pritchard
IT Security Manager
St. Charles Health System
jrpritchard@stcharleshealthcare.org

Shane Whitlatch
EVP
FairWarning, Inc.
Shane@FairWarning.com
Joining Forces for Patient Privacy: Compliance & Security Working Together

December 11, 2012

To improve the health of those we serve in a spirit of love and compassion.
Today’s Presentation

- Introduction to St. Charles Health System
- Core Principles
- People
- Process
- Technology
- Day-to-Day Operations
- FairWarning® Tips-n-Tricks
- Questions & Discussion

To improve the health of those we serve in a spirit of love and compassion.
Core Principles

INFORMATION SECURITY & PATIENT PRIVACY: Protecting patient data and respecting patient privacy are integral components of high quality care.

REGULATORY COMPLIANCE: Regulatory compliance should be an artifact of doing the right thing.
People

CAREGIVERS: Our most valuable resource

ACCOUNTABILITY: Own your actions

SET BOUNDARIES: Establish policy, monitor and enforce

COMMUNICATE: Say what you do, Do what you say
STEAL THIS POLICY CONCEPT:
“Staff may NOT look at their own medical record.”

AVOID AMBIGUITY with MUTUALLY-EXCLUSIVE ROLES:
• Caregiver
• Visitor
• Patient
REPEATABLE, CONSISTENT PROCESS:
• Caregiver Education
• Investigations & Incidents
• Corrective Actions

INFORMATION SECURITY & PROTECTING PATIENT PRIVACY is EVERYONE’S JOB:
• Caregiver
• Human Resources
• Compliance, Privacy and Legal
• IT Security

To improve the health of those we serve in a spirit of love and compassion.
BUSINESS OBJECTIVE:
Automate privacy and security monitoring for electronic access to patient medical records.

ST. CHARLES HEALTH SYSTEM INFORMATION TECHNOLOGY DEPARTMENT:
• Project Management Office (PMO)
• Enterprise Architecture (EA)
• Commitment to find appropriate technical solutions
**PROCESS**

**PROJECT PHASES**
Opportunity → Discovery → Planning → Implementation

**FRAMEWORK** for the organization to capture and prioritize initiatives in a transparent, repeatable fashion.

**ENSURES** you recognize the costs, scheduling dependencies, resource requirements and other factors necessary for making informed decisions.

*To improve the health of those we serve in a spirit of love and compassion.*
AUTOMATED PRIVACY MONITORING OPTIONS:

- Application-Specific Tools (e.g. EMR app or SSO app)
- Custom-Developed Tools
- Security Information Event Management
- FairWarning®

DISCOVERY DOCUMENT

- Requirements Matrix
- Architectural Fit
- Estimated Costs
- Resource Requirements

To improve the health of those we serve in a spirit of love and compassion.
Technology – EA & Project Planning Phase

DESIGN DOCUMENT

Vendor Selection – FairWarning®

Identify & Prioritize Audit Sources

Identify Resource Dependencies (IT, Compliance, and FairWarning®)

Finalize Project Costs

• FairWarning® Costs
• 3rd Party Costs
• Additional Infrastructure Costs
• Training Costs
Technology – Implementation Phase

Implementation Schedule
• Resource availability
• Project prioritization
• Project Managers (St. Charles Health System & FairWarning®)

Data Source Integration

Data Source Validation

Building Your FairWarning® Monitoring Team
• Compliance and Security Participation
• Invest in training

Caregiver Education & Awareness Campaigns

To improve the health of those we serve in a spirit of love and compassion.
Moving to Day-to-Day Operational Support

Focus on Quality
Start Simple and Build Operational Capacity
Know your Data Sources
• Define investigative objectives
• Ensure data sources match objectives
• Increase sources over time

Explore the Concept of “Investigative Triggers”
• Widen the scope of FairWarning® Investigation
• Widen the scope to Other Areas
• Clearly define how these would be invoked
1. Start with Simple AdHoc Queries (e.g. Self Snooping)

2. Store Refined Queries as “Saved Privacy Reports”
   - DataSource#1 Snooping (self)
   - DataSource#2 Snooping (self)
   - DataSource#X Snooping (self)

3. Automate Queries as “Alerts” for Establishing Your Investigative Framework
   - Audit & Monitoring Trail
   - Accountability

4. Use Scenarios for Viewing Aggregated Data
John R. Pritchard, PhD, GSEC, GCIH, CISSP
IT Security Manager
St. Charles Health System, Inc.
2500 NE Neff Road
Bend, Oregon 97701
Joining Forces for Patient Privacy: Compliance and IT Working Together

FairWarning® Executive Webinar Series
December 4, 2012
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.
Business Case for Privacy Monitoring

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

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

“Patient Privacy Monitoring” found to be #1 deficiency in first 20 HIPAA audits according to Office for Civil Rights

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
Leverage the FairWarning® team of privacy experts to bridge gaps in resources or expertise to implement a world-class patient privacy monitoring program.

Program highlights:

- Designed to put the care provider in a “defensible” position regarding access to electronic Protected Health Information (HIPAA Security Rule required element)
- Provide Healthcare organizations with communication and education plans/materials
- Provide proven validation/remediation processes and workflows
- Implementation of enforced policies (automated alerts) by FairWarning® staff to detect inappropriate access of ePHI
- Monitoring of enforced policies by FairWarning® staff
- Reviews and investigations of triggered enforced policies by FairWarning® staff including appropriate documentation

- Utilizes FairWarning® product technology
- **Optional service** for FairWarning® customers
- [PrivacyServices@FairWarning.com](mailto:PrivacyServices@FairWarning.com)
Contact Us

John Pritchard
IT Security Manager
St. Charles Health System
jrpritchard@stcharleshealthcare.org

Shane Whitlatch
Executive Vice President
FairWarning, Inc.
Shane@FairWarning.com