NHS Homerton Patients Can Trust That Their Privacy Is Secure...Can Yours?

FairWarning® Executive Webinar Series
12 September 2012
NHS Homerton Patients Can Trust That Their Privacy Is Secure...Can Yours?

- Meeting regulatory requirements
- Recognizing the risks - and the actions to prevent them
- How Homerton monitors patient access effectively across systems
- How Homerton is Building Patient Trust
- Why Privacy Matters
- The Importance of Audit Trails
- Q&A session
Today’s Panel

Matthew Hall
Information Governance Manager
Homerton University Hospital
Matthew.Hall@homerton.nhs.uk

Kurt J. Long
FairWarning® Founder and CEO
Kurt@FairWarning.com
NHS Homerton Patients Can Trust That Their Privacy Is Secure...
Can Yours?

Matthew Hall
Information Governance Manager
Background

- Homerton University Hospital NHS Foundation Trust
- IG Toolkit
- Data Protection Act – full compliance
- Cerner Millennium and RiO
- Trust – incidents
- Reactive audit trails
Why FairWarning®

- Provides the compliance required
- NHS experience in Scotland
- Experience of Cerner
Implementation

• Secure point-to-point VPN connection
• FairWarning® Project Manager
• Lantern Room
• Regular Updates
Implementation Methodology

FairWarning® Speed-to-Value

Organizational Adoption

<table>
<thead>
<tr>
<th>Phase 1: Kick-Off</th>
<th>Phase 2: Data Consumed</th>
<th>Phase 3: Reporting Capabilities</th>
<th>Phase 4: Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior to Kick-Off</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Welcome to FairWarning® Customer Community with Introduction by Sales Team to Implementation Team</td>
<td>Scope data sources for “Wave One” implementation</td>
<td>End Users Creating, Testing, Validating:</td>
<td>Completed “Wave One: First Productive Use” Training</td>
</tr>
<tr>
<td>Install FairWarning® Appliance</td>
<td>Use online Customer Community for shared data extraction method</td>
<td>Proactive Automatic Incident Alerts</td>
<td>End Users: 60 minutes</td>
</tr>
<tr>
<td>• Set-up in customer data center</td>
<td>Review standard data file format and deliver sample file for evaluation</td>
<td>Email Notifications of Alerts</td>
<td>Solution Admin: 30 minutes</td>
</tr>
<tr>
<td>• Establish VPN connection</td>
<td>Validate sample fields and data with End User and IT/Application staff</td>
<td>“Hands-on” Use throughout Phase 3</td>
<td>Free Ongoing Training &amp; Education</td>
</tr>
<tr>
<td>Kick-off Meeting</td>
<td>Schedule automated file delivery to FairWarning® staging directory</td>
<td>Ad Hoc Investigations across Audit Sources saving Report Results</td>
<td>• FairWarning® Online Customer Community Peer Group</td>
</tr>
<tr>
<td>• FairWarning® Project Team with Customer End User, Project Manager and Project Team</td>
<td></td>
<td></td>
<td>• Customer-led Webinars for Knowledge-sharing and Best Practices</td>
</tr>
<tr>
<td>• Online project workspace for tracking through Implementation Waves</td>
<td></td>
<td></td>
<td>• Advanced Training Sessions</td>
</tr>
<tr>
<td>• Weekly WebEx Working Sessions</td>
<td></td>
<td></td>
<td>• Product Webinars</td>
</tr>
<tr>
<td>• Access to online FairWarning® Standards Documentation and Best Practices from the Customer Community</td>
<td></td>
<td></td>
<td>• Continuing Industry Education</td>
</tr>
<tr>
<td>5 weeks duration 1-2 files from major clinical apps, 1 Authoritative User Data file</td>
<td>Iterative “Waves” of Implementation Additional Sources &amp; Reports Added Ongoing Training &amp; Maturation</td>
<td>5 weeks duration</td>
<td>• Executive Education Webinars</td>
</tr>
<tr>
<td>Data review with IT and End User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation “Wave One: First Productive Use” typically takes ~12 weeks and requires:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End User: Representative(s) for the duration of the implementation</td>
<td></td>
<td></td>
<td>Homerton University Hospital</td>
</tr>
<tr>
<td>Project Leader / PM for the duration of the implementation</td>
<td></td>
<td></td>
<td>NHS Foundation Trust</td>
</tr>
</tbody>
</table>
| IT and Application staff for a few hours per week, ~4 weeks duration | | | NHS
## Standard Field Names

<table>
<thead>
<tr>
<th>Standard Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>Datetime YYYYMMDD HH24:MM:SS</td>
<td>System timestamp indicating when the activity event was logged</td>
</tr>
<tr>
<td>User ID</td>
<td>Varchar (25)</td>
<td>System identifier of the user performing the activity</td>
</tr>
<tr>
<td>User first name</td>
<td>Varchar (25)</td>
<td>First name of the user</td>
</tr>
<tr>
<td>User last name</td>
<td>Varchar (25)</td>
<td>Last name of the user</td>
</tr>
<tr>
<td>Patient ID</td>
<td>Varchar (25)</td>
<td>Unique identifier of patient</td>
</tr>
<tr>
<td>Patient first name</td>
<td>Varchar (25)</td>
<td>First name of the patient</td>
</tr>
<tr>
<td>Patient last name</td>
<td>Varchar (25)</td>
<td>Last name of the patient</td>
</tr>
<tr>
<td>Application</td>
<td>Varchar (25)</td>
<td>The application in which the event occurred</td>
</tr>
<tr>
<td>Event Description</td>
<td>Varchar (25)</td>
<td>The detailed description of what action occurred during this event</td>
</tr>
<tr>
<td>Event Type</td>
<td>Varchar (25)</td>
<td>The category or type of event that the action during this event falls under</td>
</tr>
</tbody>
</table>
Ad Hoc Privacy Reporting
Scenarios

Privacy Scenarios

Information Security Investigations
- Corner - Activity: Patient
- Corner - Activity: User

Random Audits
- Corner - Random Audit: Patient
- Corner - Random Audit: User
Alert Detection and Automation

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cormer Discharged Patient Activity</td>
<td>Enabled</td>
<td>Security Event</td>
<td>Employees accessing discharged patients' medical records</td>
</tr>
<tr>
<td>Cormer Family Member Snooping(Same Last Name)</td>
<td>Enabled</td>
<td>HIPAA Best Practice</td>
<td>Employees accessing their family members' medical records</td>
</tr>
<tr>
<td>Cormer Self Examination</td>
<td>Enabled</td>
<td>Policy Compliance</td>
<td>Employees accessing their own medical records</td>
</tr>
<tr>
<td>Olympics</td>
<td>Enabled</td>
<td>Security Event</td>
<td>For Olympic athletes admitted, monitoring staff access</td>
</tr>
</tbody>
</table>
What’s Next

• Implementation of hardware completed
• Modify and create new Reports
• RiO and other systems
NHS Homerton Patients Can Trust That Their Privacy Is Secure...Can Yours?

*FairWarning® Executive Webinar Series*

12 September 2012
FairWarning® Patient Privacy Monitoring:
A Platform for Developing a Culture of Privacy

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

FAIR WARNING
Collaborative
Patient Privacy Monitoring

Cerner  MEDITECH
Streamline Health  Siemens

Epic  McKesson
Allscripts  Lawson
dbMotion

FairWarning
Impacting Outcomes, Revenue and Lives

Why Privacy Matters

53% of UK patients withhold medical information due to privacy concerns.

An estimated £2.7b is being invested in EHR’s, over the next 6 years.

45% of patients indicate that a care provider’s reputation for protecting privacy influences their choice to seek care from that provider.

Identity theft is one of the fastest growing crimes in the UK. Medical records are a key target for organised crime.

Regulatory and legal compliance is becoming paramount in an ever increasing competitive market: UK Data Protection Act, IGT.

Sources: New London Consulting, UK Survey; EHI Research;
What We are Seeing in Patient Privacy Monitoring

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 neighbour snooping** is a concern for care providers of all sizes and types that causes reputational damage and loss of trust.

5. **Family member snooping** has a direct impact on peoples lives.

The Importance of Audit Trails

FairWarning® Ready for Healthcare Applications
✓ Standardized data across all applications
✓ Rapid integration of data sources with advanced analytics
✓ Lower fully loaded expenses

EHR Audit Logs
and other authoritative data sources

FairWarning® Data Definition Guide

Instant Compatibility
with FairWarning®
Patient Privacy Monitoring
Learn More About FairWarning® Patient Privacy Monitoring

- **Compliance Dashboard** - Measurement of patient privacy monitoring and compliance effectiveness
- **Privacy Dashboard** - Recent investigations, enforced policies, alerts and privacy reports
- **Robust collaborative investigations** - Document the legally defensible position of the care provider
- **DoH Audit Compliance** - Direct mapping Information Governance toolkit 206 and 302 Audit requirements
- **Wide-scale support for FairWarning® Ready** - Instant compatibility with every major EHR and over 185 applications used in healthcare
- **Analytics Library** - Point and click best practice analytics, reports and administration
Resources cited in this webinar can be found at:

- [UK Patient Privacy Survey](#)
- White Paper: [Make or Break - Digital Healthcare and Privacy Reach the Tipping Point](#)
- [UK regulatory mapping document](#)
Matthew Hall
Information Governance Manager
Homerton University Hospital
Matthew.Hall@homerton.nhs.uk

Les Baker
General Manager
FairWarning® UK
Les@FairWarning.com