A Record to Rely On: A Workshop on the Intersection of Electronic Health Records, Health Law, Payment, and Oversight

November 29th, 2016

Kurt J. Long

Founder and CEO

User Activity Monitoring

- Explicit HIPAA Requirement for monitoring PHI access
- Commonly 'Insider Threat Detection'
- Detection of identity theft, medical identity theft, 'snooping', fraud
- Compromised credentials, external attacks

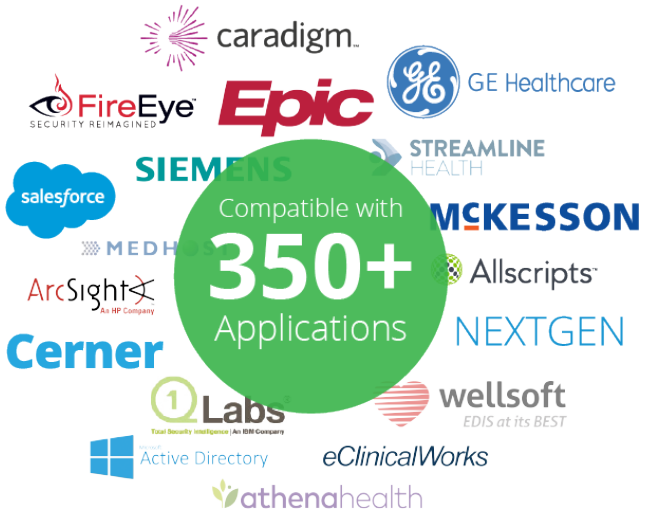
Escalation of Threats

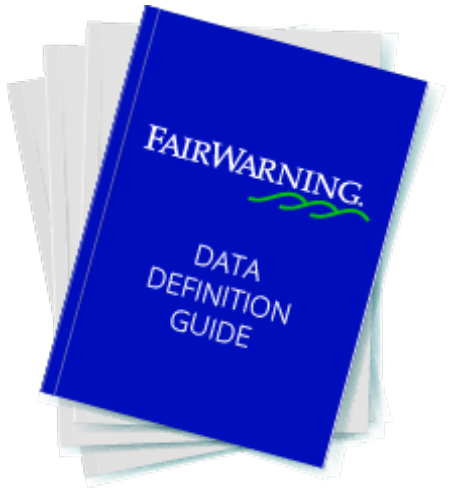
- Snooping
- Identity Theft, Medical Identity Theft
- Espionage and Politically Motivated Attacks
- Post-Breached World

Standards & Technology – User Activity Monitoring

- Lack of industry expertise and standards
- Data Definition Guide
- Guidance on appropriate program
- Enforcement

FairWarning Ready® and Data Definition Guides





EHR Audit Logs
and other authoritative data sources

FairWarning® Data Definition Guide

Instant Compatibility with FairWarning®
Patient Privacy Intelligence

*All product names, logos, and brands are property of their respective owners.