University of California SERVICES Science, Management, and Engineering

EMR: The Security-Productivity Dichotomy

Services Science, Management, Engineering

Ravi Nemana, Executive Director

Security Implications of EMR Implementation
April 28, 2006

Goals of an EMR

- **Improved efficiency & productivity**:
  - Better coordination of care, virtually and physically
    - Fewer call-backs from pharmacies
    - Reduction in “phone tag”
  - Reduction in “hunting and gathering”
  - Broad access to the chart (by more than one person at a time)
  - Better and standardized presentation of diverse data
  - Reduction in redundant data
- **Cost reduction:**
  - Reduced transcription costs
  - Reduce Labor costs
  - Reduced internal/external copying expenses
  - Malpractice insurance costs
  - Pharmacy costs
- **Revenue enhancement:**
  - Improved documentation, coding
  - Better billing
- **Improvement in quality of care**
  - Built-in protocols and reminders (including health maintenance)
  - Improved medication management, medical errors
  - Improved care coordination internally and externally (RHIOs)

Difficult Path to EMR Goals

- ➔ Many Sources and Sinks of data
  - ▶ **Integration**
  - ▶ **Interfaces**
    - ■ Require constant human intervention, monitoring, patching
    - ■ Intellectual propriety v. seamless operation
  - ▶ Many **diverse security coordination, models, access controls**
    - ■ Average 300 bed community hospital houses 200+ systems
    - ■ ~ 20 of these are “life critical”
    - ■ Many versions, patches, O/S, data formats
    - ■ Upgrades often not possible or practical
- ➔ Preserving (clinical) **productivity is paramount**
  - ▶ Responsibility of clinical productivity is shifted to IT professionals
    - ■ E.g. $750,000 for 1 wk of malware remediation in one department
    - ■ **Poor audit trailing** and tools
    - ■ **Poor automation** of security → propagation of error
  - ▶ Cultural issues impact chain of trust:
    - ■ Workflow is key– **giving/revoking rights** takes too much time / effort
    - ■ Organizational issues and HR incentives don’t support security
  - ▶ SSO and automated / context-sensitive security is not perfect

Difficult Path to EMR Goals

- Patients:
  - Largely trust the health system
  - **Assume and Expect** that security (and privacy, confidentiality, continuity) are being maintained.
  - Sue if it isn't
  - Privacy issues loom for RHIO and PHR projects
    - Selective disclosure v. incidental disclosure v. "break the glass" disclosure
- WILDCARD: **convergence of biomed and IT**
  - Risk profiling for now… but will it scale?
  - No host-based security
  - How do you patch an implantable pump? Who bears the responsibility?
- Lessons from **Katrina and Rita**
  - Biometric failure– blood and body fluids, hoarse voices, new personnel
  - Surge capacity in IT needs to support and follow surge capacity in hospital
    - The interesting role of the parking lot
  - New applications of continuity, survivable systems