Access Control!

Audit!

Why Can’t We Be Friends?

Bradley Malin, Ph.D.
Associate Professor of Biomedical Informatics, School of Medicine,
Associate Professor of Computer Science, School of Engineering
Vanderbilt University
May 16, 2012
Associated Press

Calif. hospital system settles celeb records cases
Associated Press, 07.08.11, 08:23 AM EDT

LOS ANGELES -- Years after hospital employees were accused of snooping into the medical records of celebrity patients, UCLA Health System agreed to pay an $865,000 settlement for potential violations of federal privacy laws.

The settlement that UCLA reached with federal regulators Wednesday did not name the stars involved and did not require the hospital system to admit liability.


The hospitals have agreed to report to a federal monitor on the implementation of its corrective plan over the next three years.

In a statement Thursday, UCLA said it has taken steps over the past three years to retrain staff and strengthen its computer
We Must Engineer Roles

Top-Down

Decomposition

Roles

Jobs

Work Patterns

Tasks

Permissions

Composition

Bottom-Up
Role Engineering Isn’t Easy

• You have humans in the loop
  – Security administrators
  – Human resource managers
  – Employees with specialized knowledge

• Job responsibilities and business processes are not always documented (Neumann & Strembeck, 2002)

• Informant (in)accuracy is a concern (Krakhardt, 1987)
Experience Based Access Management (EBAM)

EBAM Flavors: Access Rules Informed by Probabilities (ARIP)

We Can Reconfigure “Roles” in EHRs through Access Log Auditing

- Assess if expert-defined job titles are reasonable & refine them

Northwestern Memorial Hospital

Similar roles cause confusion

Real Role | Predicted Role | How often?
--- | --- | ---
Rehab OT | Rehab PT | 85.7%
Rehab PT | Rehab OT | 60.0%

Gripes & Next Steps

• Different providers within the same ward have different behavior!

• Different wards within the same healthcare institution have different behavior!

• Different healthcare organizations use different languages!

• Logic (i.e., access control) and AI (i.e., data mining) need to play nicely together