

# Privacy Controls for Electronic Health Records Systems

Tyrone Grandison PhD

Manager, Data Disclosure Research, Healthcare Informatics Department, IBM Almaden Research Center, 650 Harry Road, San Jose, California 95120, USA

## Motivation

- The march towards Electronic Health Records (EHRs) is progressing aggressively and appears to be unstoppable.
- A lot of technical hurdles in delivering these systems will be successively navigated.
- Unfortunately, PRIVACY is one that is often mentioned, but least addressed.

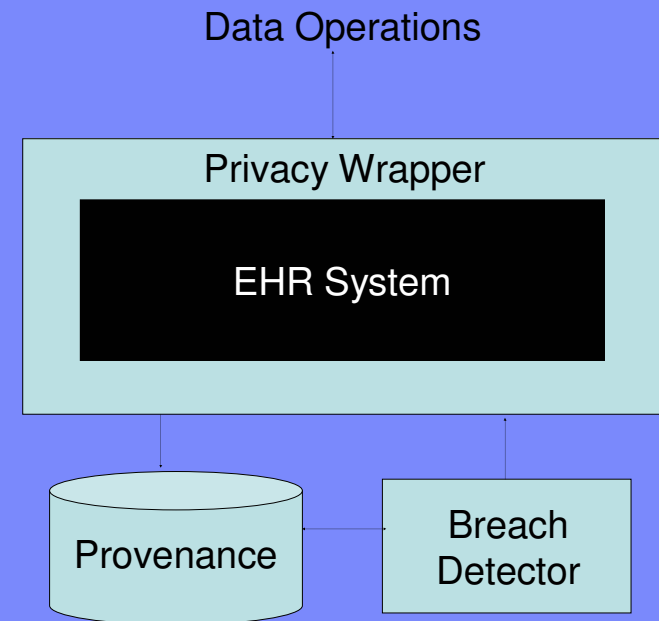
## What is it about privacy?

- The solution requires an ecosystem of business, social, technical and legislative controls. All of which re-enforce each other.
- Current thought in the privacy field has yielded *active compliance* systems.

## Problems

- Current *active compliance*-based privacy systems focus on enforcing rules when data is collected and or accessed.
- Scalability is a significant concern as privacy mandates and number of EHR apps increase and leads to unmanageable EHR systems.
- Access exceptions tend to be dominant and render current privacy controls around EHRs effectively useless.
- Highlights assumptions on location of the privacy control and the point of enforcement.
- Enforcement should be considered at disclosure, aggregation, sharing, publication, storage & retention as well.

## Solution



## Advantages

- Facilitates enforcement at multiple stages.
- Handles scenarios requiring active and retro-active support.