MedVault: Ensuring Security and Privacy for Electronic Medical Records
(http://medvault.gtisc.gatech.edu)

*Pls: GT - Doug Blough, Mustaque Ahamad, Ling Liu and Patrick Traynor
Children’s Healthcare of Atlanta- James Jose MD*
MedVault Technical Overview

Organizational VPN
- Secure EMR Storage
- Wireless Access Point
- Secure Virtualized End Devices

Personal or Community Health Record
- Verifiable and Selective Information Disclosure

Internet-based EMR Sharing
- Attribute-based Access Control
- Federated Cross-Layer Identity and Access Management

Other External Users
(patients, patient surrogates, community physicians, emergency responders, etc)

Other EMR Provider

Other EMR Provider

Other EMR Provider

Other EMR Provider
Securing Health Information on End Devices

- Patients and care givers will access information on end devices such as smart phones
- End devices such as sensors produce health information
- End devices will help in user awareness, control and consent
- Mobile devices will becoming increasing targets of attacks as they manipulate sensitive data
- Loss or theft of end devices
MedVault Approach for Securing Information on End Devices

- Threat model for mHealth technologies
- Research Challenges
  - Creating trusted execution environments for healthcare applications
    - Kernel hardening and virtualization based isolation
  - Monitored read and writes
    - Cryptographic solutions to ensure that data access cannot bypass trusted remote monitor
    - Leveraging health monitoring
  - Secure user consent detection
    - User or malware generated request?
Questions??