Big Health Care Data
(MedVault: Ensuring Security and Privacy for Electronic Medical Records)

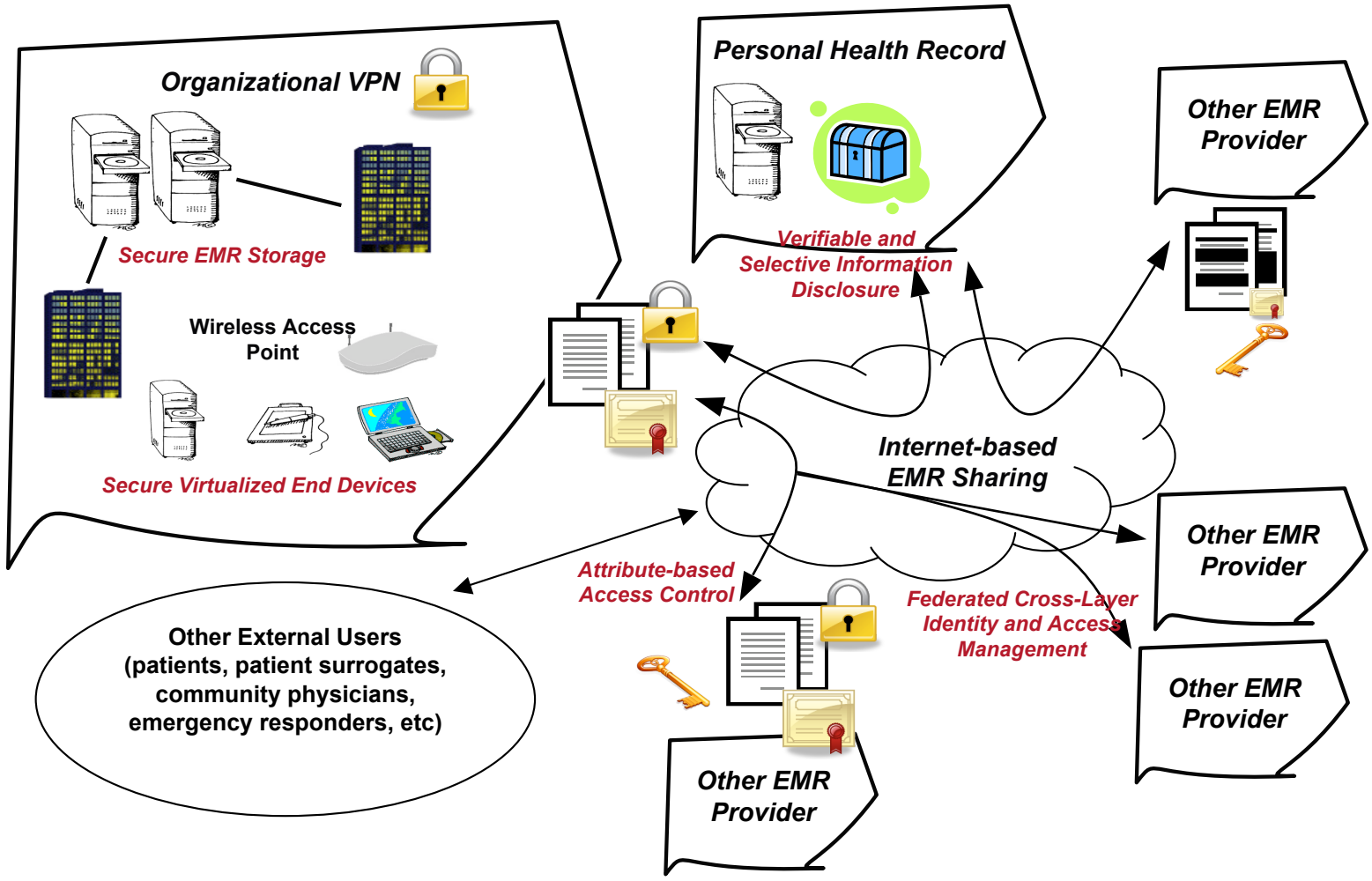
Doug Blough
(doug.blough@ece.gatech.edu)

Joint work with: *Mustaque Ahamad, Ling Liu, Praveen Chopra*

Georgia Institute of Technology
Children's Healthcare of Atlanta

Primary Sponsor: National Science Foundation
Additional Sponsors: I3P, Nortel

MedVault Technical Overview



Trends in Medical Data

- Wide-spread sharing of health care organizations' EMR data with external entities, e.g. patients, community physicians, EMT personnel, other health care organizations, public health officials, medical researchers
  - Cross domain data search/analysis
- Third-party services for users' maintenance and control of their medical data, e.g. Google Health, Microsoft Health Vault
- Generation of large volumes of medical data from non-traditional sources, e.g. home-based health care and portable medical devices

Challenges and Selected Approaches

- Authorization and access control in federated environments
  - Credential-based (attribute-based) systems
- Privacy: cross-correlation attacks mean stripping obvious personally identifiable information is not sufficient
  - Data obfuscation to group data into sets of a minimum size
  - Privacy vs. usability
- Identity
  - Uniquely identifying patients without use of globally unique identifiers such as SSNs
    - Attribute similarity metrics
  - Identification of individuals accessing medical data
    - Auditing + secure binding of credentials to credential owners
- PHR services with data verifiability and selective disclosure
  - Novel types/uses of redactable signatures

Challenge: Dealing with Real-Time Sensor Data