Securing Sensitive Health Information in the U.S. Health Care System: Past, Present and Future

Doug Blough, Georgia Tech

In collaboration with: *M. Ahamad, L. Liu,* Georgia Tech
and *J. Saltz, T. Kurc,* Emory

Graduate student contributors: *D. Bauer, J. Brown, D. Mashima, A. Mohan,* Georgia Tech

Georgia Institute of Technology

cercs

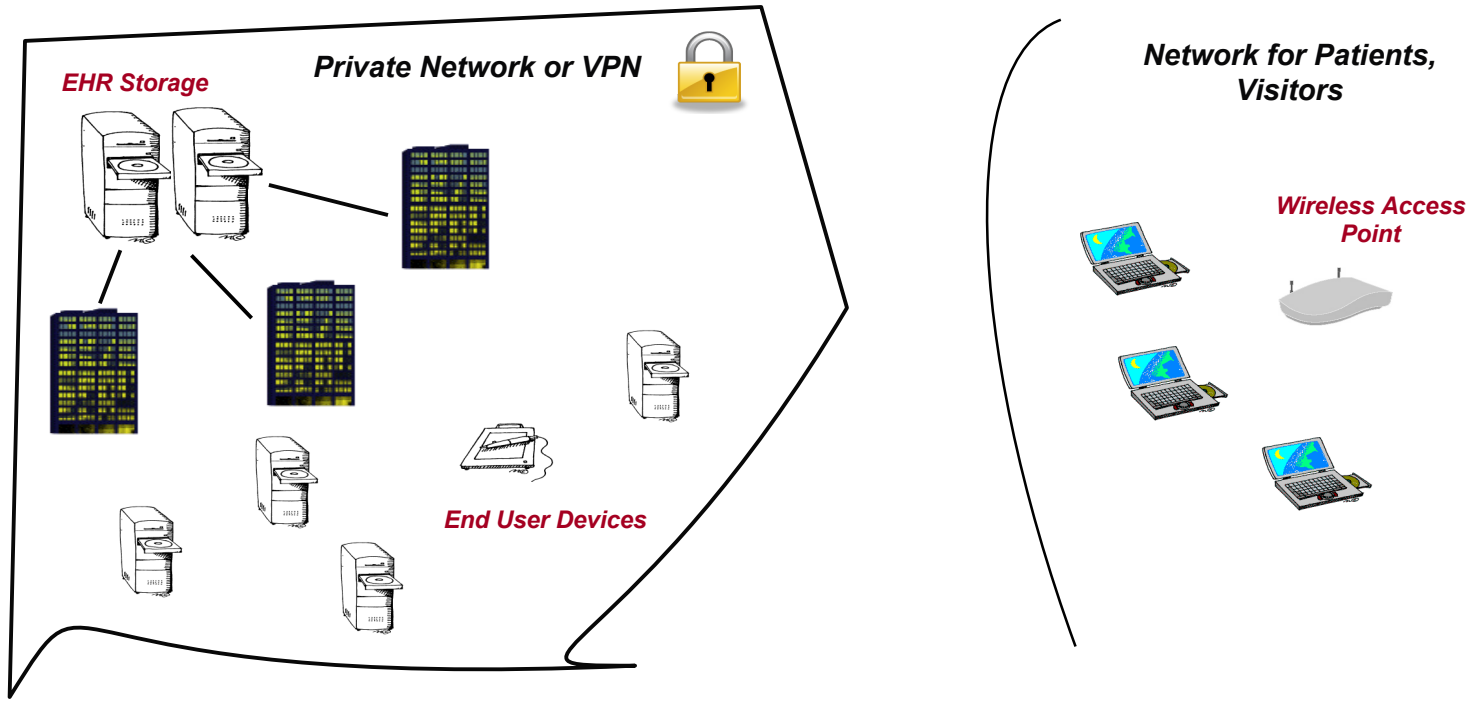
GEORGIA TECH INFORMATION SECURITY CENTER

CS Research in Health IT

- ***Personal health*** or ***mobile health:*** home health devices and monitoring, applications to assist with personal health maintenance/improvement, social networking for health, etc.

- ***Health IT in the health system:*** software-controlled medical devices in hospitals and doctor's offices, *electronic health record (EHR) repositories and exchanges*

Past: Closed Health Systems Architecture



- On-site access only – no external connections allowed (only exception is pushing of billing info)
- Primary threat – insider attack

Typical Security Model for Closed Systems

- ***No access control*** – any health professional (doctor, nurse, technician) can see all records about all patients; ***tension between care, security***
- ***Logging*** of all EHR accesses
- ***"Random" auditing*** is performed (in practice, auditing is typically performed on high profile patients or when a complaint has been filed)
- ***Training*** of all staff on policy – EHR info to be accessed only for legitimate medical purposes
- ***Accountability*** – serious consequences, up to and including dismissal, for policy breaches

Representative Incidents in Closed Systems

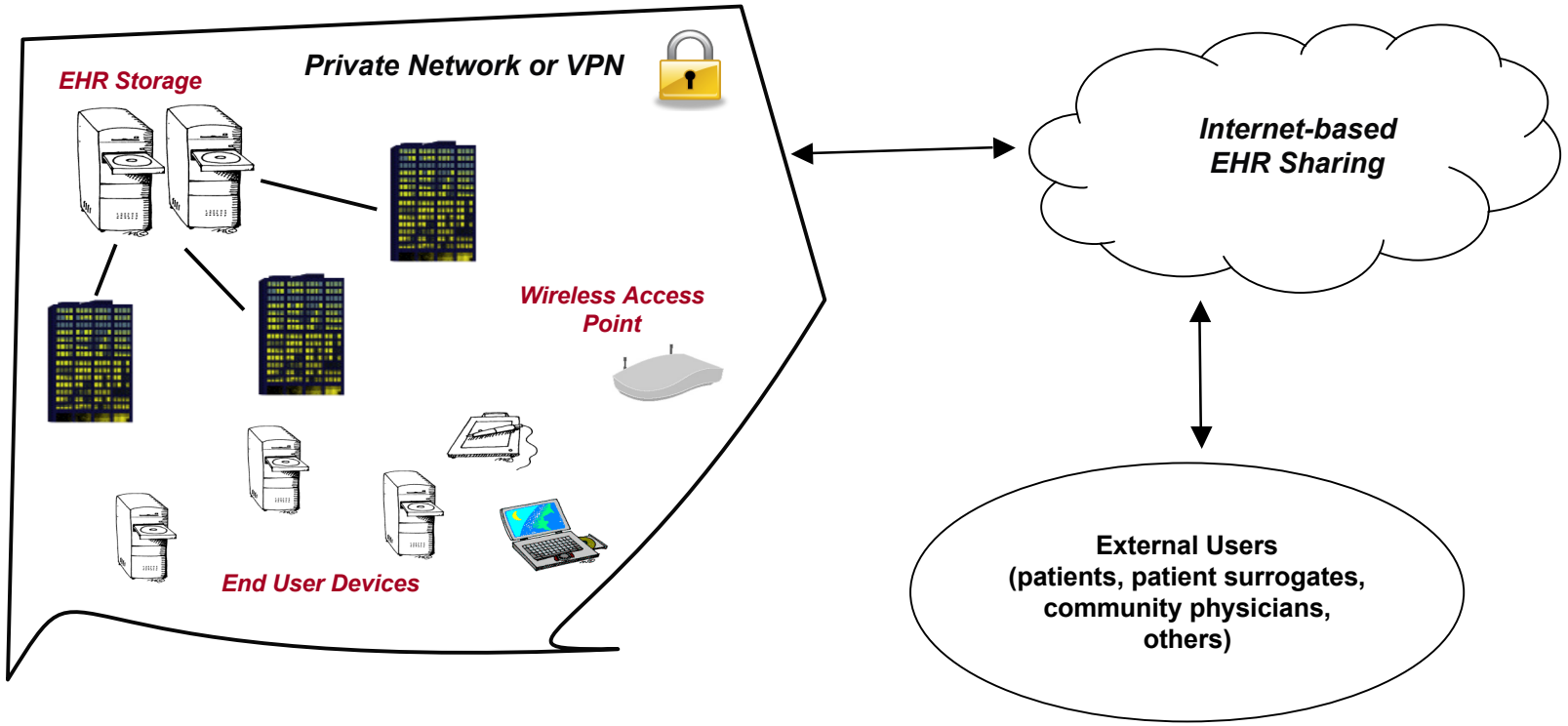
- ***Lost or stolen components:*** laptops, tapes, servers
  - In 2006, an Indiana man stole a server containing records of 900,000 patients and attempted to extort money from AIG by threatening to release the information on the Internet

- ***Human error***
  - From 1999-2005, Kaiser Permanente posted records of 150 patients on a misconfigured Web site accessible to the public
  - In 2008, a contractor for Grady Hospital in Atlanta posted records of 45 patients on a public Web site for several weeks
  - In 2007, records of 900,000 soldiers, govt. employees, and family members were posted on an SAIC server on the Internet

Representative Incidents, continued

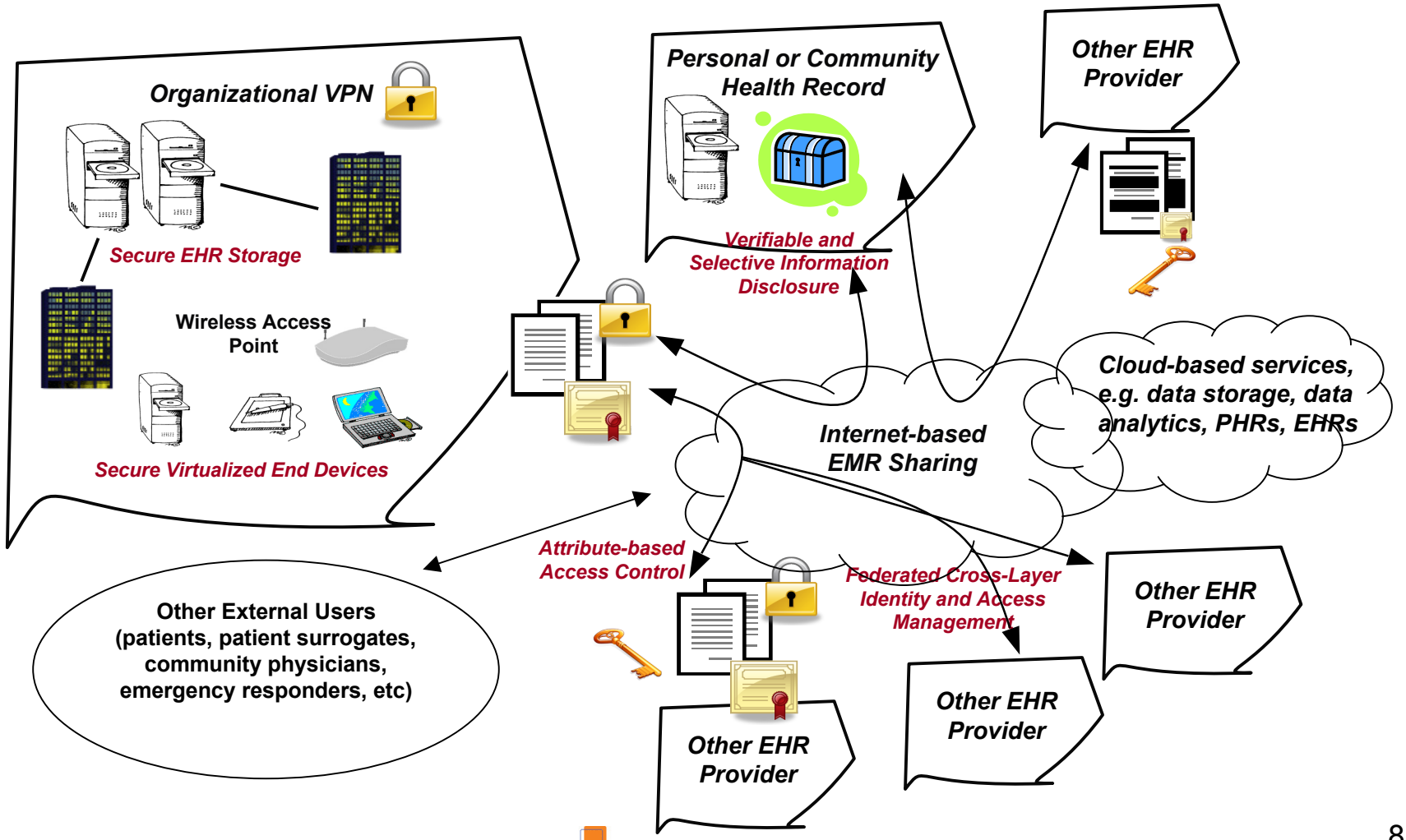
- ***Deliberate internal breaches*** – usually small-scale: curiosity, revenge, blackmail, divorce/custody disputes, etc.
  - In 2009, two Kaiser Permanente employees were fired, 16 resigned, and 9 were otherwise disciplined for accessing the records of Nadya Suleman and her children
  - In Jan. 2011, 3 clinical support staff and 1 nurse at Tucson Univ. Medical Center were fired for unauthorized accesses to records of Gabrielle Giffords and other shooting victims
  - No reliable statistics on this category, many cases likely go undetected

Present: Limited External Access



- Common patient uses: access to test results; communication with doctors, nurses; limited views of EHR info; prescription refills
- Currently, limited health information exchange, usually within a highly localized region and between systems from same vendor, is occurring

(Near) Future: Large-Scale Health Information Exchange (HIE)



Georgia Institute of Technology

cercs

GEORGIA TECH INFORMATION SECURITY CENTER

Emerging Threat Examples

- ***Insider threat explosion:*** if closed system access model is extended to HIE, insiders will include most health care professionals in the US, public health officials, and many others
- ***Malware:*** in 2009, 300 Windows boxes controlling MRI machines in the US were found to be infected with the Conficker worm
- ***Monetization of stolen health information:*** in Oct. 2010, the largest Medicare fraud in history, carried out by a large organized crime syndicate, was announced
  - identities of thousands of Medicare beneficiaries and licensed physicians were stolen
  - perpetrators used stolen info to bill Medicare for services never provided
  - $163M in fraudulent billings through 118 phony clinics in 25 states

Examples of Security and Privacy Research Challenges

- Transparent situationally-aware access control
- Anomaly detection
- Provenance – both for auditing and compliance
- Dynamic detection and resolution of policy conflicts
- Metadata privacy – inference attacks
- Identity management: both users (health care professionals) and non-users (patients)
- E-consent
- Dealing with widely distributed health records and information authenticity
- Intrusion detection/tolerance, malware analysis and detection, etc.

MedVault Research Threads

- Transparent situationally-aware access control
- Verifiable and redactable health records
- Monitoring of health record accesses

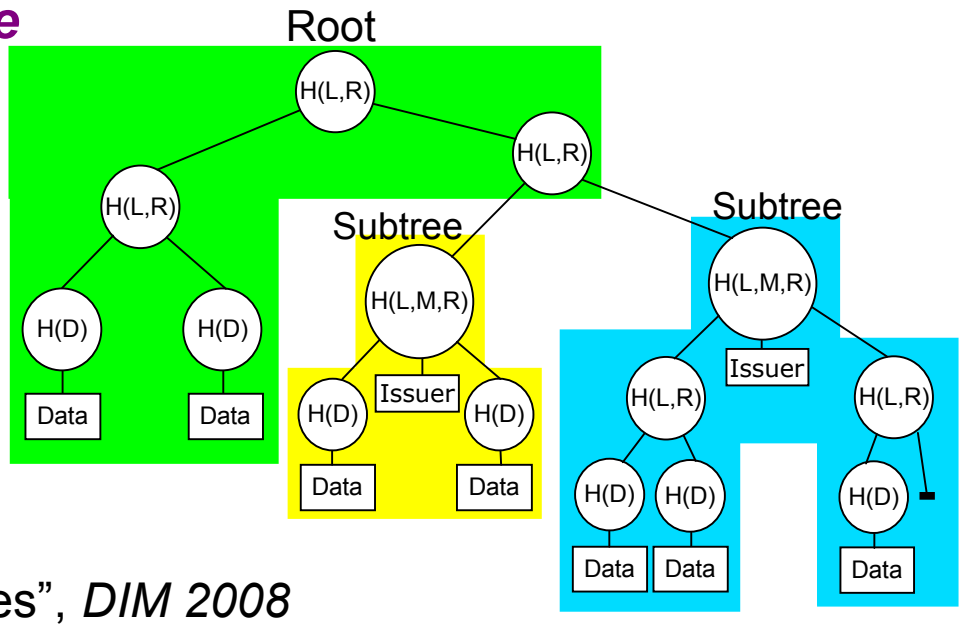
Transparent situationally-aware access control

- ***Transparent situational awareness*** through collection of large number of trusted attributes, both static and dynamic
  - "Attribute Trust", *2008 Int'l Conf on Privacy Security and Trust*

- ***Adaptive policy-driven authorization*** mechanisms that adjust to current situational context and combine policies from multiple stakeholders - patient, health care provider, regulatory agencies, HIE operator, etc.
  - "Dynamic policy conflict resolution", *IDTrust 2010*
  - "Detection of conflicts and inconsistencies in taxonomy-based policies", *BIBM 2011*

Verifiable and redactable health records

- Sources of health information sign records with a ***redactable signature***
- Records are shared with another entity, e.g. patient or other provider
- Other entity can pass along records while ***redacting sensitive information***
- ***Integrity*** of unredacted information and ***verifiability*** of sources are provided
  - "Multi-authority redactable signatures", *DIM 2008*
  - "Redactable signatures with data disclosure dependencies", *WPES 2009*
  - "Verifiable and redactable medical documents", to be submitted



Georgia Institute of Technology

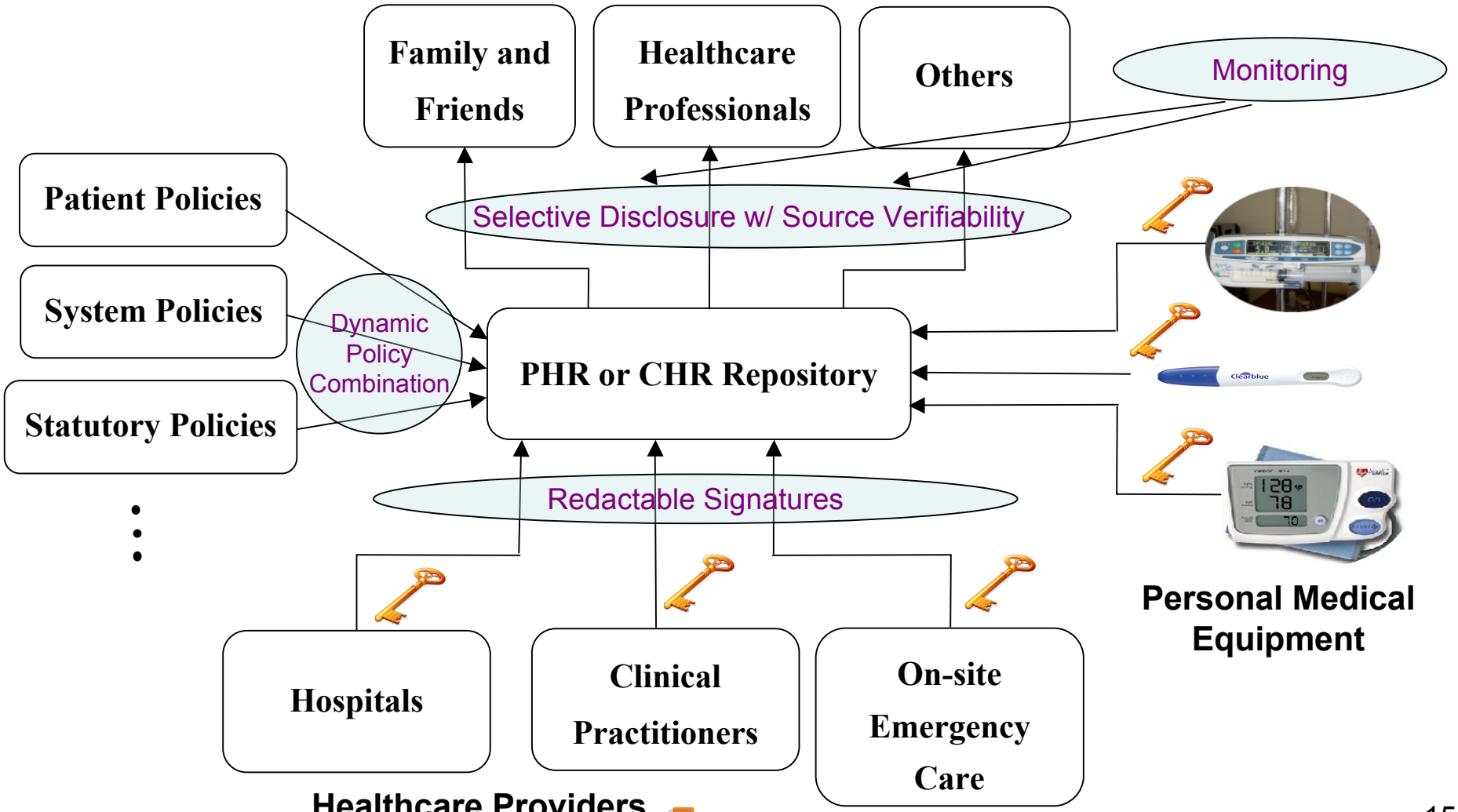
cercs

GEORGIA TECH INFORMATION SECURITY CENTER

Monitoring of health record accesses

- Monitoring of credential usage, e.g. to detect stolen physician's credentials, *DIM 2009*
- Monitoring health record accesses and reporting to patients how information is being used, *IHI 2012*

A Patient-centric, Source-verifiable Health Records Repository



Georgia Institute of Technology

cercs

GEORGIA TECH INFORMATION SECURITY CENTER

Current and Future Research

- BDD-based formal evaluation of policies - consistency, completeness, safety, other security properties
- Detection of possible inference attack vulnerabilities through correlation analyses of sensitive and non-sensitive elements and analysis of policy inconsistencies
- Implementation and evaluation of attribute-based policy-driven security in the Atlanta Clinical and Translational Sciences Institute Biomedical Information Exchange
- Security for cloud-based health services

http://medvault.gtisc.gatech.edu

Questions??