Future of Privacy in Health IT

ISPAB Briefing, May 30, 2012

Gerald Beuchelt

Health in the 21st Century

Follow us on Twitter
MITREHealth

MITRE

MITRE

Mission Statement

As a public interest company, MITRE works in partnership with the government, applying systems engineering and advanced technology to address issues of critical national importance.

MITRE's Focus on Health IT

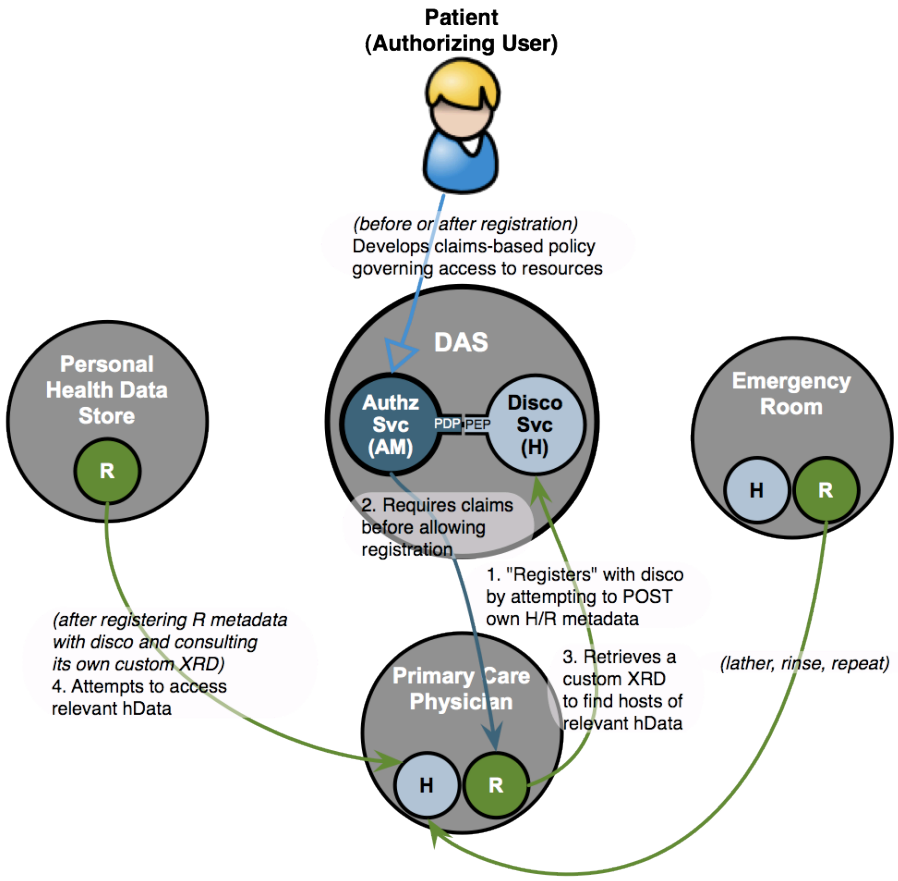
- Through this work, MITRE manages the critical tradeoffs between agile cybersecurity and timely data sharing and analysis. Examples include:
  - hData Standards for Electronic Health Information
  - Kairon Patient Consent Management
  - popHealth Population Health Monitoring
- Demonstrate simple, secure, and standards-based health information exchange
  - Apply proven web technologies to health domain for secure and private exchange
  - Apply hData using Patient Data Server (PDS)
  - Inform possible new standards

Patient-Centric Privacy

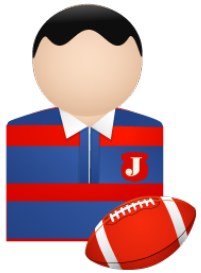
- **Basic access control available today through limited privacy controls**
  - **Individual Clinical Documents can be marked as sensitive**
  - **Coarse granularity**
- **Web Based Privacy and Access Management**
  - **Looking at web-centric authentication and authorization protocols**
  - **Focus on developing PII and HIPAA compliant profile**
- **Future requirements**
  - **Minimally: individual entry-level granularity**
  - **Ideally: XML node based access control**

Data Sharing Aspects: Patient Centric

- **Resource-orientation enables application of user-centric identity management to the clinical domain**
  - **Patient can allow advanced EHR systems into a personal *health data federation***
  - **Patient-managed with privacy-preserving policy defaults**
- **Enables patient-moderated cross-organizational data sharing**



Future Patient-Centric Scenario

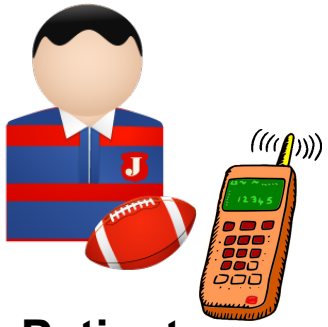


Patient

Patient registers with Discovery and Authorization Service

Discovery and Authorization

PCP Visit



Patient

Patient sees PCP during regular visit

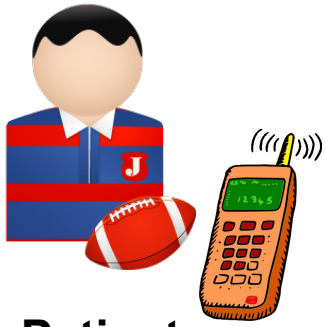
Everything is ok

Discovery and Authorization

Patient authorizes PCP system to federate with patient discovery service

PCP

Emergency: Sports Accident



Patient

Sees emergency room surgeon after sports accident.

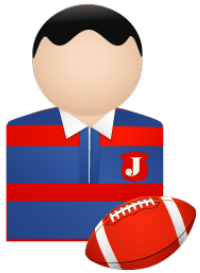
ER Surgeon

Surgeon EHR system is authorized; discovers existing systems from patient service

Discovery and Authorization

PCP

Data Retrieval and Subscription



Patient

Sees emergency room after a sports accident.

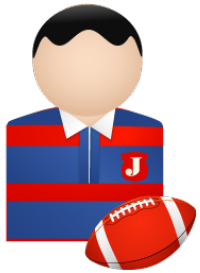
ER Surgeon

Gets the relevant data from the PCP EHR system. Also subscribes to PCP EHR system.

Discovery and Authorization

PCP

Data Retrieval and Subscription



Patient

Performs procedure and prescribes new medication

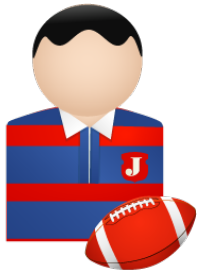
ER Surgeon

Updates local records with new data

Discovery and Authorization

PCP

Discovery Service Check



Patient

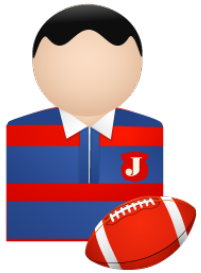
ER Surgeon

Discovery and Authorization

Discovers new system from surgeon and updates subscription

PCP

PCP System Update



Patient

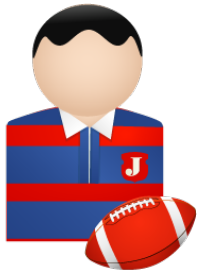
ER Surgeon

Subscribes to data for patient from new system and updates records

Discovery and Authorization

PCP

Follow Up Visit



Patient

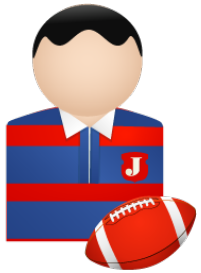
Sees PCP for follow up; PCP prescribes new medication

ER Surgeon

Discovery and Authorization

PCP

Near Real Time Update



Patient

ER Surgeon

Updates data via subscription;

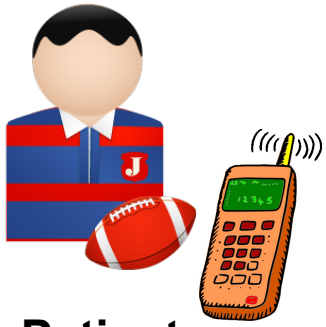
obtains new medications

Discovery and

Authorization

PCP

Near Real Time Notification



Patient

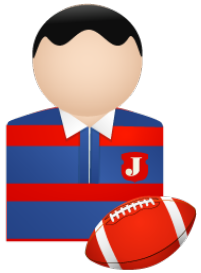
ER Surgeon

Warns patient and PCP about potential problems with medication

Discovery and Authorization

PCP

Patient-Centric Provider Change



Patient

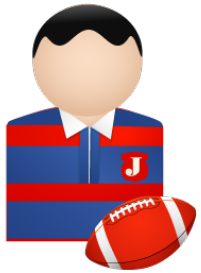
ER Surgeon

Discovery and Authorization

Patient decides to change surgeon; updates authorization service to deny future access

PCP

Subscription Access Revoked



Patient

ER Surgeon

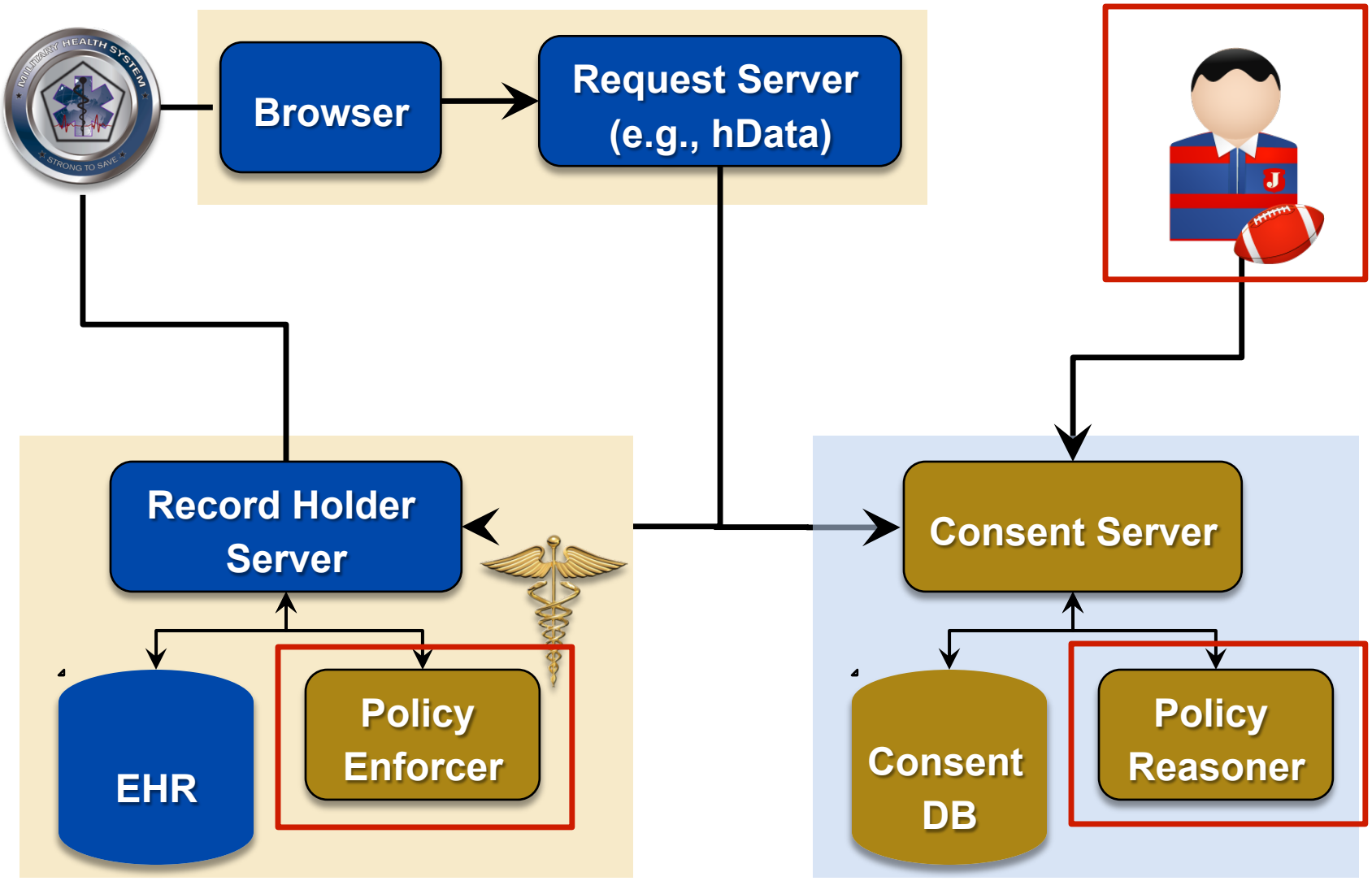
Access tokens are revoked;

surgeon system cannot get more data

Discovery and Authorization

PCP

Interoperability with Patient Consent



Example for Privacy and Consent Problems

- Patient wants to hide his mental health condition from his dentist
  - Dentist should not be able to infer from clinical data that patient has mental health problem
- Dentist wants to prescribe pain killer
  - Drug-drug interaction between Lithium and Ibuprofen that requires close monitoring of blood Lithium levels
- If dentist knows about Lithium, he knows about mental health problems

Conclusions

- Today's privacy control systems are very limited
  - Limited automatic cross-organizational data sharing
  - Fallback to human-managed access control decision
  - Limited or no patient-facilitated privacy controls
- Future systems will be capable of
  - Enable patient access control and consent for inter-organizational data sharing
  - Fully automated identity-based discovery of EHR services
  - Semantically consistent application of patient preferences

More Information

- **MITRE Center for Transforming Health**

http://www.mitre.org/work/health/

Public Release Approvals: 09-2805, 09-4511,09-4513, 09-4557, 09-5212, 10-0100, 12-2251