

Strategic Healthcare IT Advanced Research Projects on Security (SHARPS)

SHARPS Project and ILHIE Prototype
June 26, 2013



Strategic Health IT Advanced Research Projects (SHARP)



- **SHARP Area 1** – Security and Health Information Technology (SHARPS), University of Illinois
- **SHARP Area 2** – Patient-Centered Cognitive Support (SHARPC), University of Texas at Houston
- **SHARP Area 3** – Health Care Application and Network Design (SMART), Harvard University
- **SHARP Area 4** – Secondary Use of EHR Information (SHARPN), Mayo Clinic of Medicine
- **NIH Affiliate** – Medical Device “Plug-and-Play” Interoperability Program (MDSHARP), Massachusetts General Hospital, supported by NIH/NBIB Quantum Grant

The Six Challenges



SIX RESEARCH CHALLENGES

FOR THE SECURITY AND PRIVACY OF HEALTH INFORMATION TECHNOLOGY

1. Access controls and audit
2. Encryption and trusted base
3. Automated policy
4. Mobile health (mHealth)
5. Identification and authentication and
6. Data segmentation and de-identification

1. Access Controls and Audit



- Complex and safety critical workflows make it difficult to assign least privileges to Health Care Organization (HCO) personnel.
- Typical strategy: use audit to catch problems after the fact.
- Problems: too reactive and insufficiently scalable.
 - ▣ New threats: large scale fraud
 - ▣ New ways to share records: Health Information Exchanges (HIEs)
- Research aim: provide more automation so large numbers of accesses can be reviewed by computer algorithms
 - ▣ Leave final decisions to humans

2. Encryption and Trusted Base



- HCOs are struggling with many changes in the systems they need to secure.
 - Bring Your Own Device (BYOD)
 - Cloud services
 - HIE systems
 - Patient portals
- How is it possible to define and manage a practical trusted base?
- Typical strategy: use standard encryption techniques to control risk and define the trusted base.
- Other strategies: use novel types of encryption and tamper-resistant hardware.
- New problems: Advanced Persistent Threats (APTs)

3. Automated Policy



- New demands to share Electronic Health Records (EHRs) with partners and through HIEs.
- Current techniques are too manual and informal.
- Ideally compliance to legal and enterprise sharing rules can be expressed precisely and maintained automatically.
- Integration with existing EHR systems is essential for effective deployment.
- Research: extending ontologies to include key concepts and expressing access rules over these concepts in a precise and modular way.

4. Mobile Health (mHealth)



- Mobile and remote devices are creating a changing landscape for managing health information
 - ▣ Intelligent medical implants
 - ▣ Cell phones that sense and process health data
 - ▣ New sensors and actuators work on the body
 - ▣ Sensors in homes
- Data are collected everywhere and by everyone!
- Rapid change in technology and regulatory environment
- Blurred distinction between medical devices and EHR

5. Identification and Authentication



Username: `cgunter` **Identification**
Password: `*****` **Authentication**

- Misidentifying a patient is a serious risk
 - ▣ Within an HCO
 - ▣ And between distinct HCOs
- There are new and worrisome threats for authentication
 - ▣ Medical identity theft
 - ▣ Large scale fraud based on hundreds of appropriated identities
- More steps are being done by computer
- A larger pool of people will need to be identified in HIEs
- Research challenge: a systematic and scientific approach to identification and authentication techniques

Science of Security



- How can we balance security against other factors like usability and safety?
- Long-standing case study is authentication.
- Key techniques
 - Secret: something you know (password, key, ...)
 - Token: something you have (smart card, ...)
 - Biometric: something you are (fingerprint, retinal scan,...)
 - Multi-factor: combinations of these like card and PIN
- Security staff fight an ongoing battle with employees in many HCOs
- How does one prove that a security precaution is worth the inconvenience it causes?
 - Compare: proving the value of measures against infection

6. Data Segmentation and De-Identification

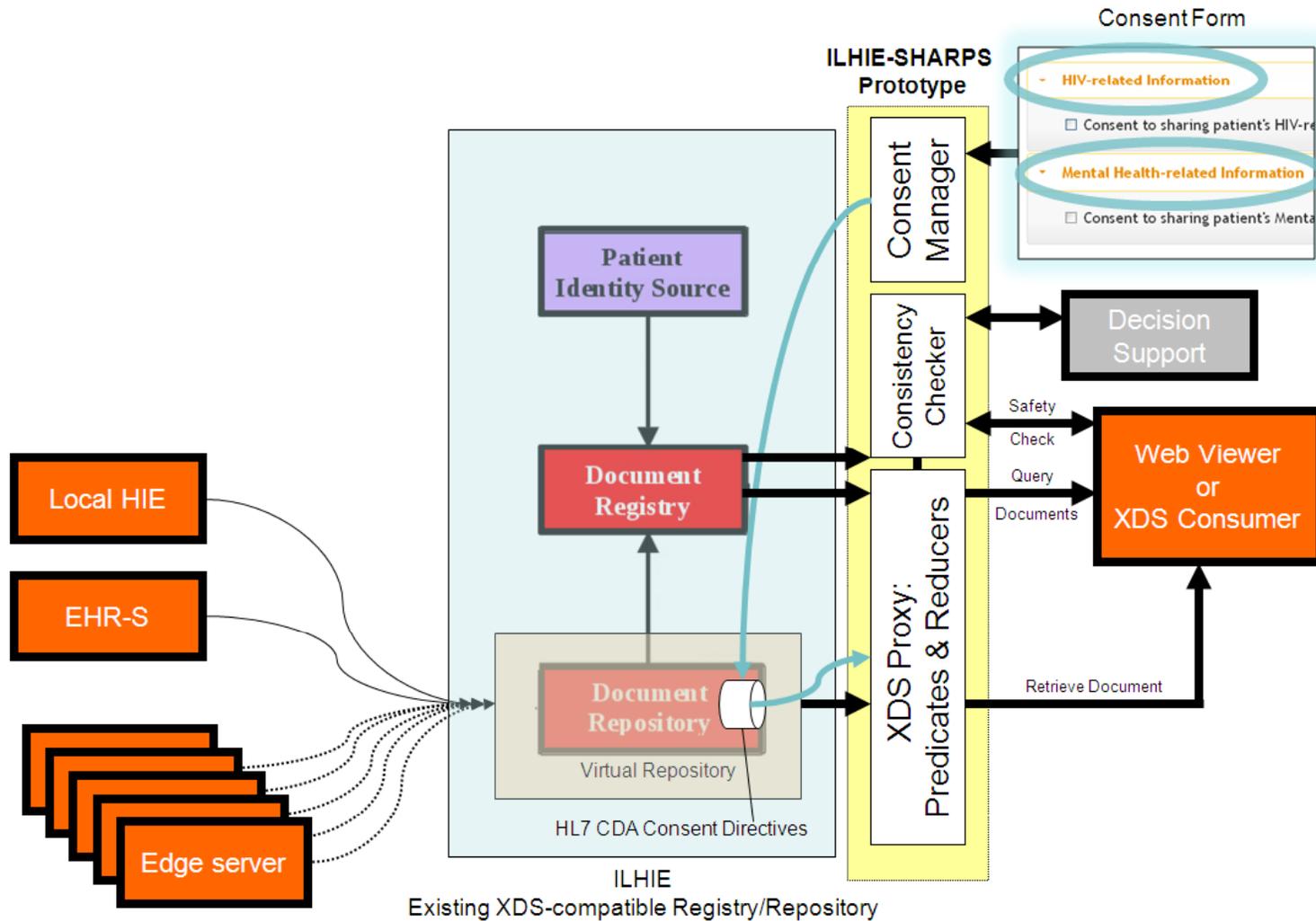


- Patients feel that some types of health data are especially sensitive: records related to mental health, drug abuse, genetics, sexually transmitted diseases, and others
- There is a desire to transmit this type of information only when necessary
- Data segmentation: breaking the EHR into parts
- This is a hard problem in many cases
 - ▣ History with de-identification (segmenting the personally identifying parts of the record)
 - ▣ Case study: HIV
- How do we balance feasibility, privacy, and clinical impact?
- Research challenge: how to segment and measure

- Data Segmentation for Privacy prototype for HIE
- Automated enforcement of patient preferences
- Standards-based, open source Clinical Decision Support model
- Platform to collaboratively develop, test, compare, and share data segmentation strategies



ILHIE Prototype Architecture



- **Predicate:**
 - Identify if a clinical document has a particular type of sensitive data in it
- **Reducer:**
 - Redact portions of the clinical document until corresponding predicate is satisfied
- **Safety Checker:**
 - Check care plan against non-redacted clinical document



Clinical Decision Support in ILHIE Prototype

