**Introduction:** Sharing of sensitive sensory information in medical studies and mobile healthcare

**Sharing is Useful**
- **Medical Studies**
  - Continuous collection of patient’s physiological signals in their daily life.
  - Sharing of medical sensor data as well as contextual information.
- **Mobile Healthcare**
  - 24/7 remote patient monitoring
  - Personal healthcare assistance

**Problem Description:** Balancing individual privacy and information utility

**Privacy vs. Utility**
- **Individual’s Privacy**
  - Data Contributors want to control who can access their information and how much of it others can obtain.
  - Data Contributors also want to control where their data are stored.
- **Data Utility**
  - Medical researcher require a certain quality of data for their studies.
  - To provide a certain level of quality of mobile health services at least some information needs to be shared.

**Goals**
- **Principle of Least Sharing**
  - Need to provide mechanisms for sharing only what is needed to achieve a certain utility.
- **Behavioral Privacy: beyond privacy of identity**
  - Privacy with sensory information
  - Sensory information can be used to infer various behavioral information as well as identity.
  - Need to protect “what you do” as well as “who you are”

**Proposed Solution:** Data sharing architecture with fine-grained access control, remote data stores, data obfuscation, and utility assessment

**SensorSafe Architecture**

**Key Features**
- **Fine-Grained Access Control with Privacy Rules**
  - Various combination of conditions (data consumer, location, time, sensor, and value) determine access permissions (allow, deny, and modify)
  - User interface for defining privacy rules
- **Remote Data Stores**
  - Institutional or personal data stores.
  - Point of data storage is closer to data contributors.
  - Efficiently store sensor waveform data.
- **Data Obfuscation**
  - Performed on remote data stores.
  - Restrict inferences that can be drawn using sensor data.
- **Utility Assessment**
  - Analyze data contributor’s privacy rules.
  - Compare and match with desired data quality of a certain service.
  - A medical researcher organizes a study and recruit people with proper privacy rules which provide desired utility.

**Design Details**

**Control Server**
- User authentication and administrative jobs
- Query processing
- Privacy rule processing
- Utility assessment
- Data visualization
  - Store
    - Privacy rules
    - Remote data store mappings
  - API
    - Query
    - Data upload request
    - Privacy rules

**Remote Data Stores**
- Data representation
  - Wave segments
- Support for non-numeric data
- Data obfuscation engine
- API
  - Data upload/download

**Prototype Implementation**
- Centralized version of SensorSafe
- Access control and data store

**Planned Evaluation**
- Case studies: conducting medical study, mobile healthcare application
- User studies: feedback about UI, privacy mechanisms
- Performance
  - Control Server: central bottleneck. Load balancing.
  - Overhead of query/rule processing on the control server
  - Overhead of data obfuscation on the remote data stores