TRUMP: A Trusted Mobile Platform for Self-Management of Chronic Illness in Rural Areas

Chris Burnett, Peter Edwards, Timothy J. Norman, Liang Chen, Yogachandran Rahulamathavan, Mariesha Jaffray and Edoardo Pignotti

University of Aberdeen

cburnett@abdn.ac.uk

Introduction

- Chronic illness requires significant allocation of healthcare resources
  - over 80% of GP consultations
  - type 2 diabetes: 10% of total NHS budget (7% prescribing budget)
- Rural areas are more challenging...
  - limited resources
  - difficult to access
  - disjoint, ad-hoc, multi-agency care
- Rural populations: 1 in 5 in UK (29% in Scotland) & 71% in India

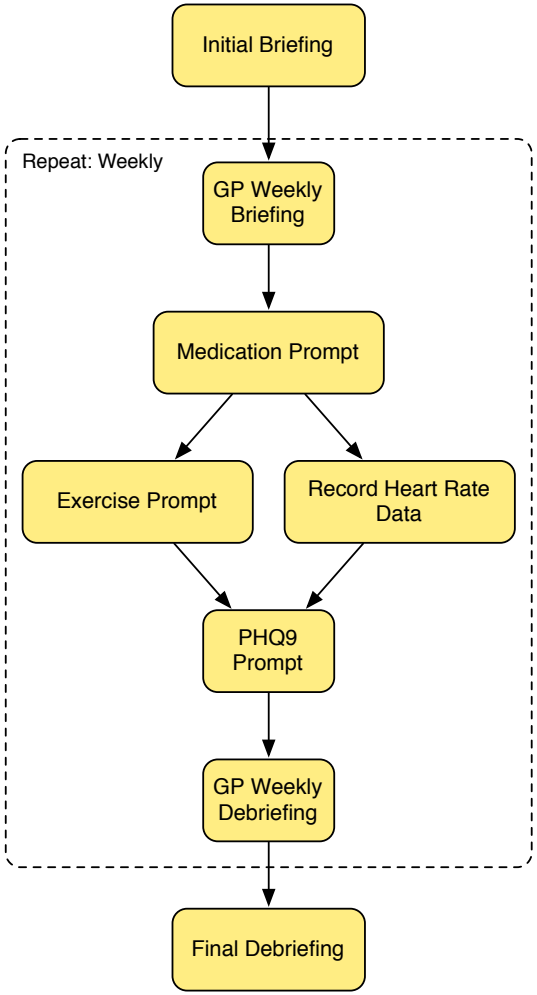
Self-management Interventions

- Some chronic illnesses can be self-managed by patients
- Design of *novel, innovative* interventions
- Collection of sensitive personal information
  - location traces, sleep patterns, diet, medication, peer communication, mood diaries
  - monitored and adjusted by healthcare professionals
- Complex flows of information
- Continued adherence is crucial
- Our focus: addressing **diabetes and depression** in rural areas of **UK and India**

Mobile Devices

- Mobile phones present a potential platform for delivery of SMIs
  - Easily carried by patient
  - Can be augmented by sensors (e.g. via Bluetooth)
  - GPS and accelerometers
  - Specialised sensor packages (e.g. Nike FuelBand)

Example Intervention



Problem

- Existing SMI approaches not concerned with trust/privacy issues
- Patient consent obtained at outset
- Policy remains fixed
- Little transparency for patients
- Existing electronic healthcare systems view patient as a data subject, not owner

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style

News › Society › NHS

NHS patient records may be shared with private companies

David Cameron to argue that giving NHS data to life science researchers will make it easier to develop and test new drugs

Andrew Sparrow Political correspondent
guardian.co.uk, Sunday 4 December 2011 12.35 GMT

Trust issues

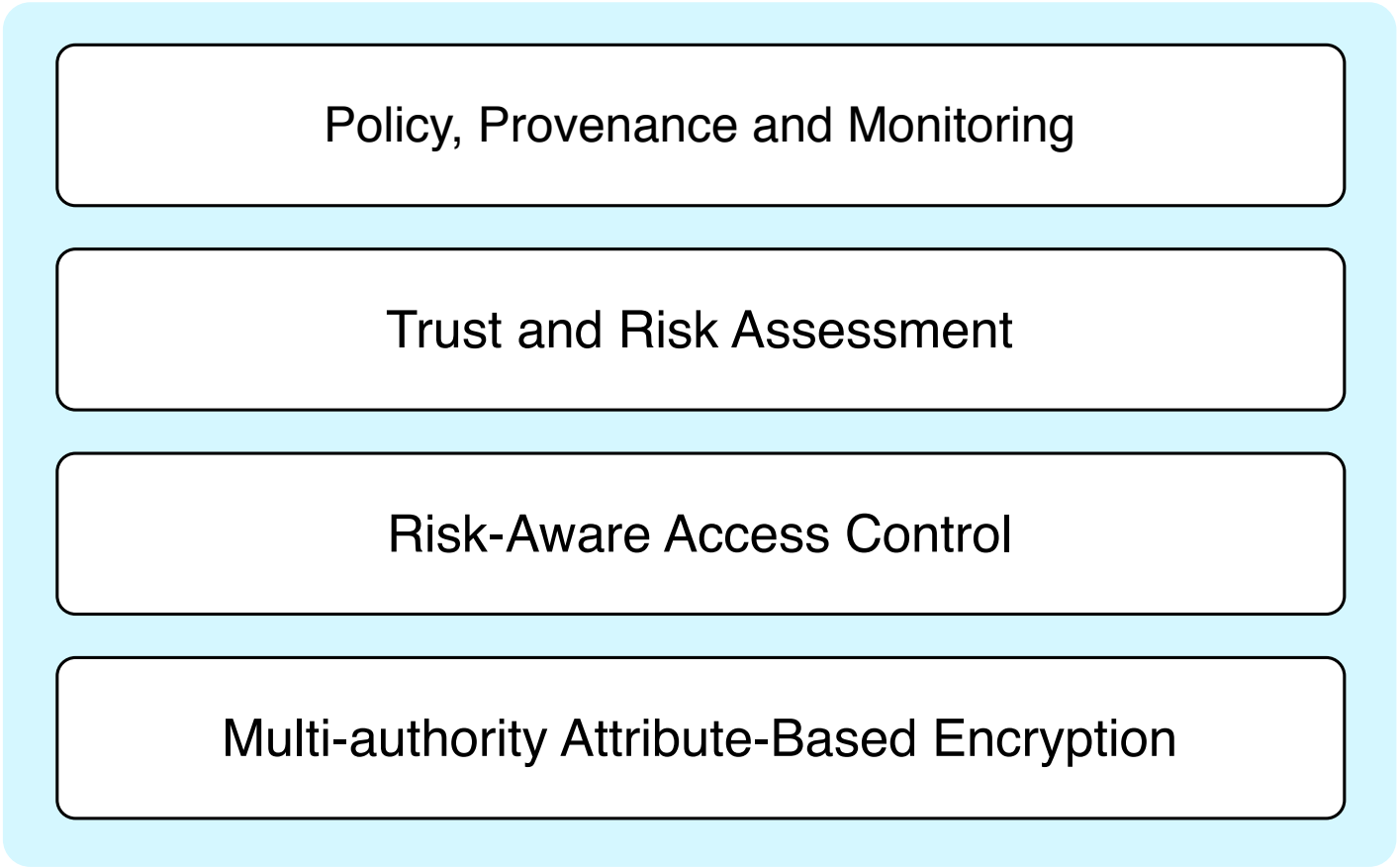
- User acceptance *critical* to effective interventions
- Platform must be *trusted* by all users
- Without trust. . .
  - patients may not be willing to provide accurate information or carry out prescribed actions
  - clinicians may lack confidence in patient-provided information
- Actors may change over time - need to quickly establish trust *between actors*
- Need to accept diverse IT landscape
  - need for unforeseeable emergency access
  - "creative" bypassing of access restrictions

Defining Trust

Important to carefully distinguish various *notions* of trust:

- User trust in system
  - transparency, predictability
- Trust between users
  - history of adherence to policies, consistency
- User trust in information
  - reliability, quality, provenance of information source
- System trust in users
  - authentication, authorisation

Trustworthy Intervention Platform



Policies

- Users must be able to express *privacy policies* about what must/can/must not be done with their data, by whom
- Privacy controls can impede interventions
- Intervention policies mandating/prohibiting actions
- System should assist users in specifying privacy policies which maintain intervention *feasibility*
- *Feasibility:* no conflicts between various user policies blocks all action

Provenance

Record of people, institutions, entities and activities involved in producing, influencing, or delivering a piece of data

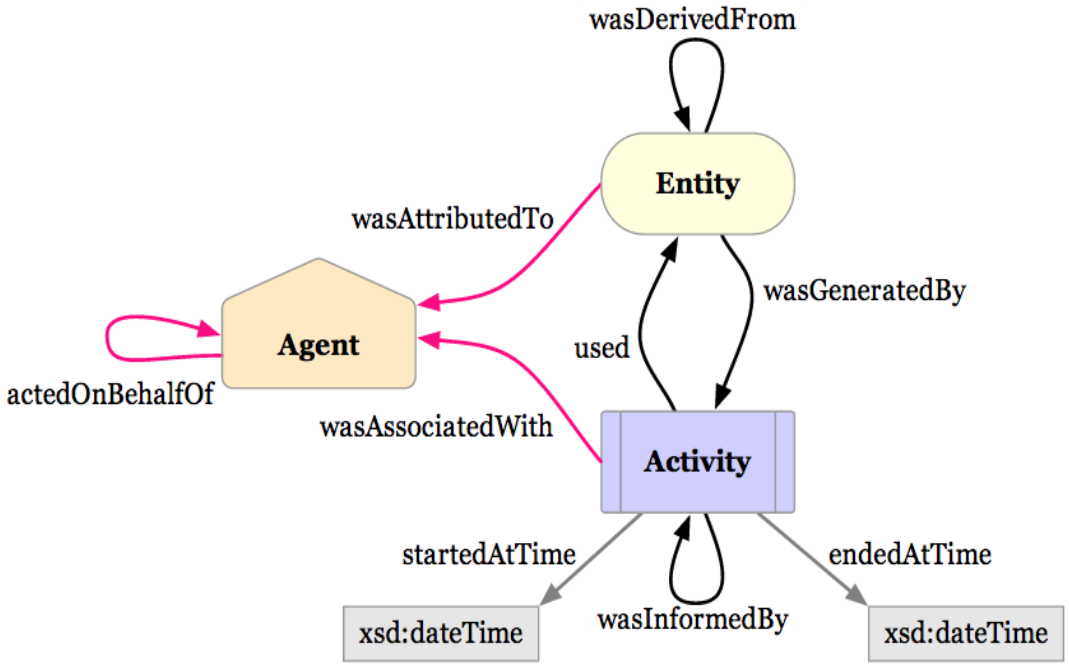


Figure: Core W3C PROV-O model

Provenance

- Allows system to be *audited*
- Identify intervention "breakdown" points
- Evaluate reliability of self-reported information
  - e.g. user reports going for a jog, GPS trace agrees, while heart rate monitor reports coincident resting heart rate
- Policies can apply to provenance layer also:
  - Restricting access to provenance elements
  - Obligating sharing actions (e.g. for notifications)

Trust Assessment

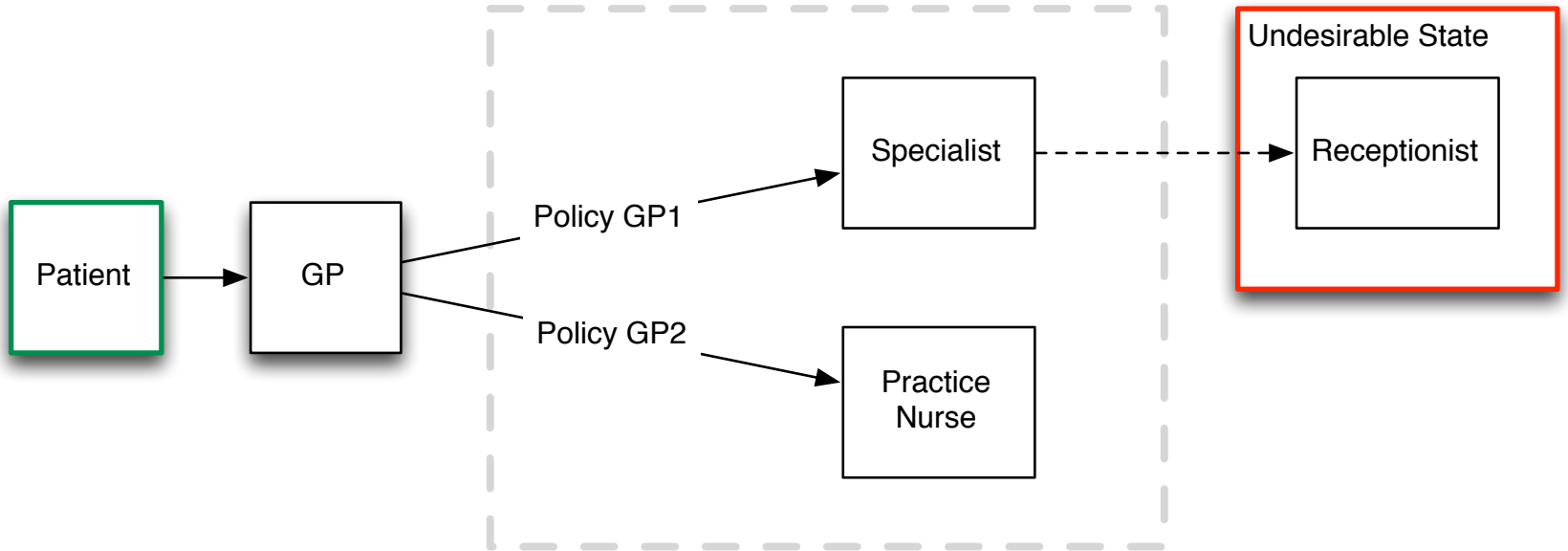
Given the decision about whether to grant or deny access:

- **Trust:** probability that some actor will behave as expected when entrusted with some privileged access
- Simple expectation: that actor will abide by agreed policies
  - Historical provenance record can be used to identify policy violations
  - Probabilistic models to predict likelihood of future violation
  - Stereotypical models allow trust to be learned about *feature* sets, as well as individuals

$$trusts(userA, userB, weeklyReportDeadline, 0.79)$$
$$trusts(Specialist, Nurse, weeklyReportDeadline, 0.84)$$

Trust Assessment

- Need to consider more complex information flows
- *Responsibility* for violations



How do we update trust in the GP now?

Risk-Aware Access Control

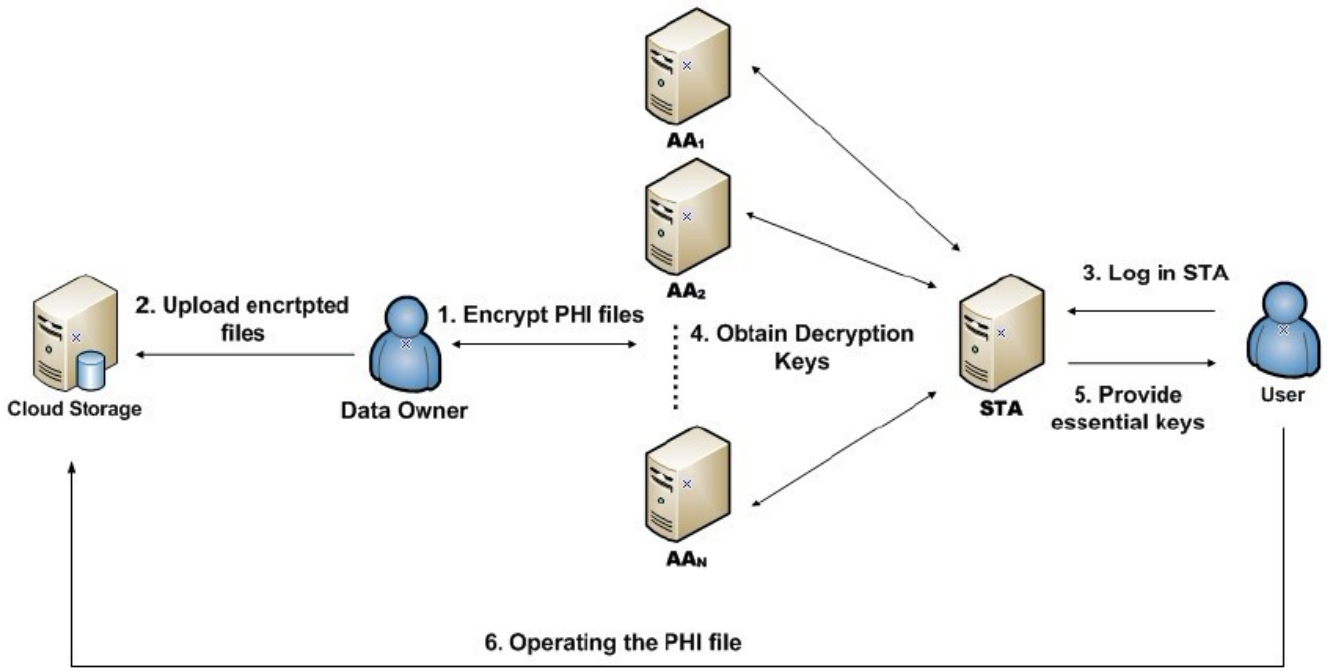
- Addresses need for sharing information in dynamic environment
  - Decision to allow or deny access is based on risk
  - Risks associated with both allowing and denying access
- RAAC is more permissive than traditional access control
  - Some risky or exceptional access is allowed, given that it is below a *risk threshold*
  - Risk mitigation strategies bring perceived risk within acceptable thresholds

Risk Mitigation and Obligations

- Obligations are typical risk mitigation methods
- Fulfilment can be required before or after access is granted
  - system obligations (enforceable)
  - user obligations (unenforceable)
- Incentive mechanisms
- Degree of trust w.r.t. fulfilling mitigations should determine perceived risk reduction
- Fulfilling obligations could affect trust and risk in future interactions

Low-Complexity Encryption

- Encryption allows *enforcement* of access control decisions
- Some overhead can be outsourced to semi-trusted servers
- Particularly suited to mobile devices with power constraints



Dynamic attributes

- Currently investigating possibility of *dynamic* attributes
- Attributes based on parts of the request context
  - time/date - e.g. within office hours
  - request location - e.g. at home
- Decryption only possible with correct attributes and in correct *context*

For more information

L. Fei, Y. Rahulamathavan, R. Muttukrishnan, R, Phan. "Low Complexity Multi-authority Attribute Based Encryption Scheme for Mobile Cloud Computing," Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on, pp.573,577, 2013

itemize

How should privacy and trust advice be presented to users

- we do want to encourage adherence...
- usable simplifications/discretisations

How do we capture and represent:

- user policies
- expectations
- risk thresholds

Conclusions

- Self-management interventions have great potential to improve quality-of-life for sufferers of chronic illnesses
- Rural areas challenging, but provide opportunities for real impact
- Mobile devices provide an attractive platform, but introduce a number of trust issues
  - provenance of and trust in data from various sources (inc. patient)
  - trust between actors to follow agreed policies
  - trust in systems to maintain privacy of sensitive data
- Socio-technical challenge

Too long; didn't read

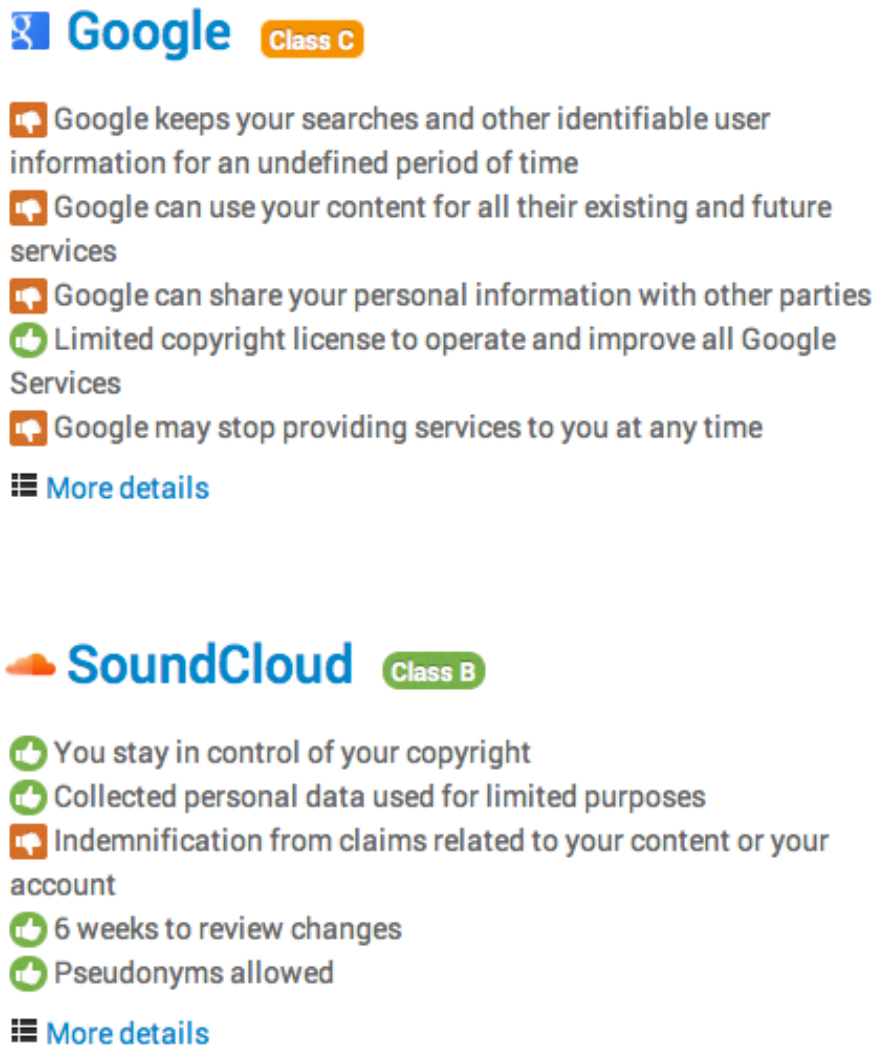


Figure: Terms of Service; Didn't Read (http://tosdr.org)