mHealth: Privacy Challenges in Smartphone-based Personal Health Records and a Conceptual Model for Privacy Management

eHealth Workshop – 28-29 Oct 2014
Middlesex University, London, UK

Edeh Esther Omegero and Carlisle George,
Middlesex University, UK

Summary

- Privacy
- Importance of Privacy in Health Information
- Privacy and eHealth/mHealth
- mHealth
- Personal Health Records (PHR)
- Personal Health Information flow
- Privacy, Smartphones, sPHR
- mHealth and Privacy Issues
- SmartPhone PHRs and Privacy Challenges
- An mHealth Privacy Framework
- sPHR and privacy
- Developing new guidelines and an sPHR privacy management model

Privacy

- Right to privacy is a "fundamental human right" (ECHR)
  - Right of anonymity
  - Right to be left alone
  - Freedom from intrusion
  - Right to control when, how, and to what extent one's personal information is collected, shared and disclosed
- Facilitates other values including principles of personhood: personal autonomy, individuality, respect, dignity and worth as human beings (Pritts, 2008).

Importance of Privacy in Health Information

- Health data = 'the epitome of private information' – reveals vulnerabilities of a person. (Wicks, 2013).
- Medical diagnosis, medication history, genetic information, treatments, medical images, sexual preference, psychological profiles, mental health, etc.
- Need privacy to ensure that such information remains private.
- Z v Finland – ECHR ruling 22009/93[1997]

Privacy and eHealth/mHealth

- Digitization of health records have brought privacy challenges, specific to accessing and sharing these electronic health records. (Dumortier and Verhenneman, 2013)
- New innovative ways of delivering healthcare (e.g. mHealth) has brought new privacy challenges (Reuters, 2013).

mHealth

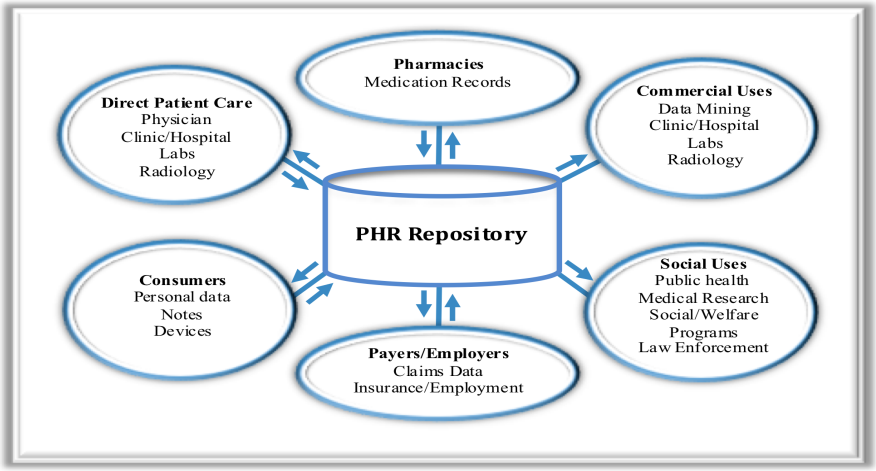
- An important sub-segment of eHealth
- Uses mobile communications technology and devices in the delivery of healthcare related services (PwC, 2012).
- Continuous, pervasive healthcare anytime and anywhere. (Lindeman, 2011).
- Spans:
  - direct-to-individual consumer and interactive patient communications to
  - more complex computer-based systems facilitating and coordinating patient care and management.

(Lindeman, 2011)

Personal Health Records (PHR)

- The tailoring of healthcare delivery to be more patient-centred gave rise to personal health records (PHR).
- Allows patients to have more control over the handling of their personal health information.
- Platform for patients to have their complete health records accessible to them and to whoever they decide to share it with (Steele et al, 2012).
- **Smartphones** are increasingly being used as a local repository for PHRs.
  - allows patients to store, transfer and access their health records using various computing and mobile technologies

Personal Health Information flow



Adapted from: Li 2013

Privacy, Smartphones, sPHR

- Use of smartphones for PHRs introduces the problem of ensuring that the personal health information (PHI) it contains is protected from privacy violations.
  - potential of gathering huge amount of data and reporting it to the interested party without the users' knowledge.
  - medical identity theft is the fastest growing form of identity theft.
  - victims are left with unpaid medical bills, damage to their reputation or worse misdiagnosed based on another person's health information.
- sPHR faces an enormous challenge due to risk of unauthorised disclosure.
  - Studies shows smartphones PHR applications are increasingly being developed without consideration of the privacy implications to the users. No privacy settings

mHealth and Privacy Issues
(Li, 2013)

- Duality of Patients' empowerment and privacy risk.
- Privacy violations (innocently or maliciously) by health care professionals.
- Vulnerability to unauthorized access from hacking or device being stolen.
- Potential access and misuse by certain data recipients – pharmaceutical companies, marketers, insurers, employers.

SmartPhone PHRs and Privacy Challenges

- **Threats from Smartphone Platform** – apps developers have access to users' data without the users' knowledge or prior authorisation (Ahmed, 2009)
- **Access threats** – data owner may fail to assert rights, insiders may want to 'peek' at user's PHI out of curiosity or intention to harm. Outsiders may access content.
- **Device Compromise** – features e.g. communication protocols for text messaging, email, packet switching for internet access offer potential for hacking. Lost or stolen devices.

An mHealth Privacy Framework
10 principles - (Avancha et al 2012)

- Openness and Transparency
- Purpose Specification
- Collection limitation and data minimization
- Use limitation
- Individual participation and control
- Data quality and integrity
- Security safeguards and controls
- Accountability and remedies
- Individual access to data
- Anonymity of presence

mHealth privacy framework

- Addresses most of the privacy issues affecting different kinds of electronic records in mHealth systems.
- But it cannot be generally applied.
- Need to tailor it to suit specific environments or platforms.
- Objective of study – develop privacy guidelines and a conceptual model for managing privacy specific to smartphone PHR applications.

sPHR and privacy

- In order to gain end-users trust, which is an essential factor that can foster the wide adoption of sPHR, there is the need address these privacy challenges and protect sPHR from privacy breaches.
- Possible solution to addressing these privacy issues:
  - ensure that privacy principles, guidelines, or recommendations are adhered to or incorporated from the initial design stage sPHR applications.

New guidelines and a new privacy management model for sPHRs

Research Methodology

- Survey questionnaire was used to gather data for requirements analysis.
- Evaluation of three existing mobile PHRs using the recommended published PHRs evaluation criteria by both by Altarum Research Group (2007) and Martino and Ahuja (2010).
- Soft Systems Methodology (SSM) for the development process of the proposed conceptual privacy management model for sPHR.
- Scenario based evaluation of the proposed privacy management model for sPHR.

Users' Requirements

- They want to be aware of the collection, use and disclosure of the PHI
- They want to be able to control the use, access and disclosure of their PHI
- They want privacy assurance when using the sPHR app

PHRs policy evaluation (CapzulePHR, ClarusPHR and on Patient PHR).

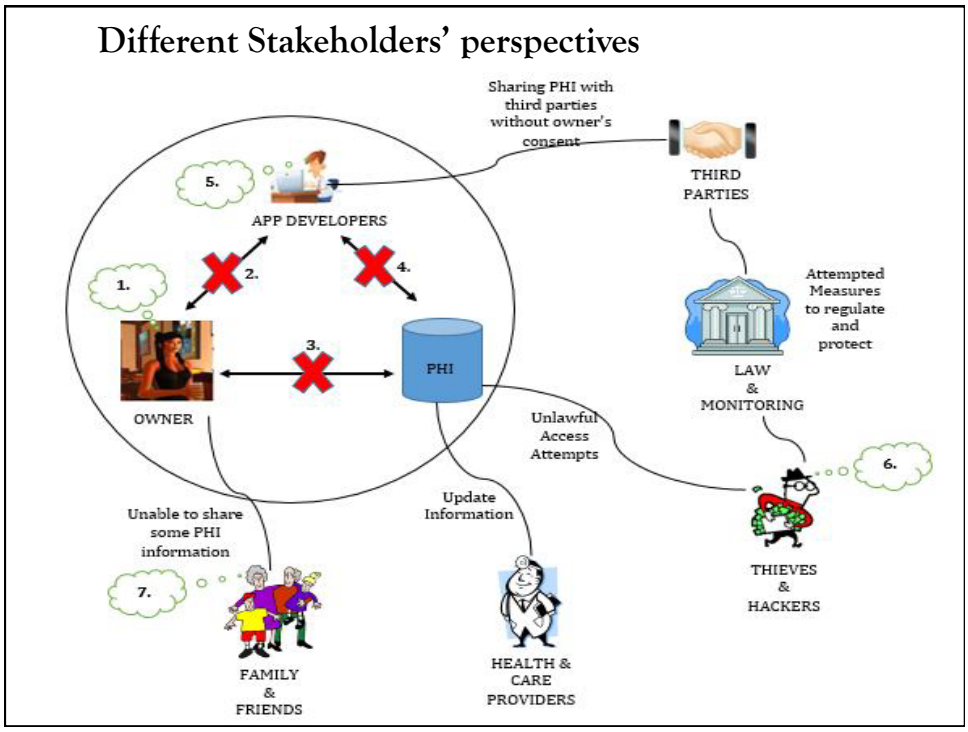
- Ease of Access
- Readability
- Communication between the PHR provider and the User
- Collection, sharing and disclosure of user's data
- Adherence to regulation, guidelines or codes (Transparency)
- Access and data management
- Bundled with security policies

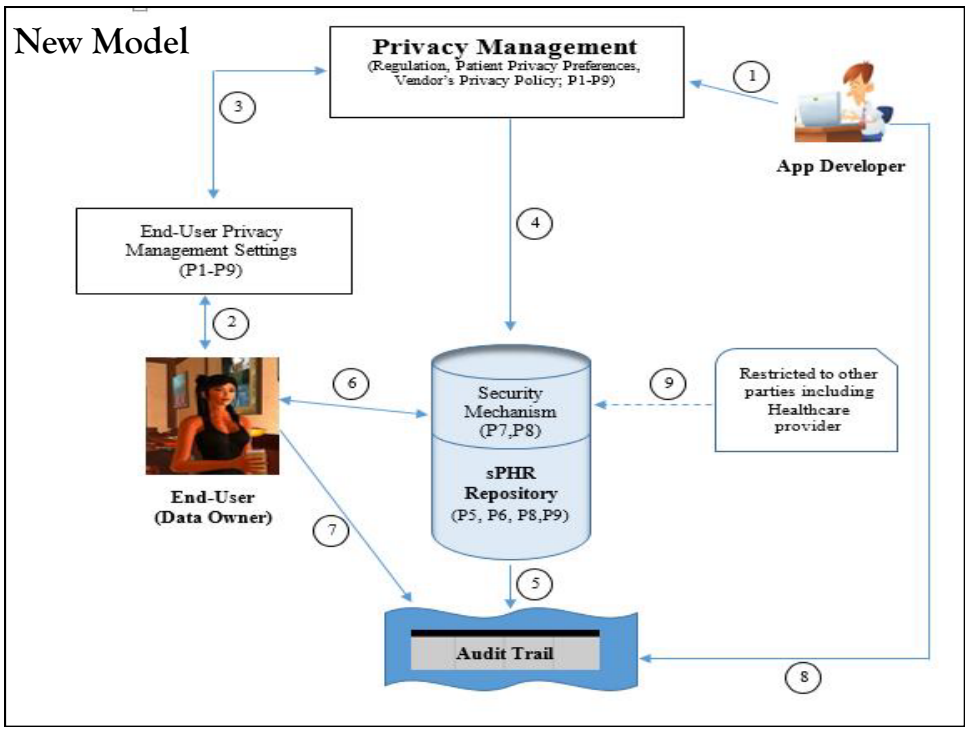
New recommended 9 Privacy guidelines for sPHR

- P1. Inform users on how their data will be processed.
- P2. Enable users to control their data via informed consent
- P3. Ensure ease of data modification by users
- P4. Have an easy to use interface
- P5. Limit collection of PHI
- P6. Limit to pre-specified purposes
- P7. Ensure access authentication
- P8. Provide adequate security mechanisms
- P9. Enable remote management

Development of a Privacy Management Model for sPHR

- Use of the **CATWOE** technique, part of SSM – to identify what the problems are, and how the solution will affect end-users and other parties. (Checkland and Poulter, 2006).
- **C**ustomer – Owner of PHI
- **A**ctors – Health Care providers (& partners), sPHR owners, sPHR developers, family
- **T**ransformations – easy , effective and secure persoal health data management
- **W**eltanschauung – All medical health data should be secure
- **O**wner – of the PHI
- **E**nvironment – law/Gov't agencies, regulators and monitoring agencies, hackers and thieves.


Different Stakeholders' perspectives
Sharing PHI with third parties without owner's consent
THIRD PARTIES
5.
APP DEVELOPERS
1.
2.
4.
3.
PHI
OWNER
Attempted Measures to regulate and protect
LAW & MONITORING
Unlawful Access Attempts
6.
THIEVES & HACKERS
Update Information
Unable to share some PHI information
7.
FAMILY & FRIENDS
HEALTH & CARE PROVIDERS


New Model
Privacy Management
(Regulation, Patient Privacy Preferences, Vendor's Privacy Policy; P1-P9)
1
App Developer
3
End-User Privacy Management Settings (P1-P9)
4
2
6
Security Mechanism (P7,P8)
9
Restricted to other parties including Healthcare provider
End-User (Data Owner)
sPHR Repository (P5, P6, P8,P9)
7
5
Audit Trail
8

Evaluation

- Scenario based - description of scenario that raises a series of questions to illustrate the problem.
- This was followed by a solution using the model.
- Result – the model effectively addressed the identified users' requirements.

Bibliography

- Ahmed, M.H (2009) Threats to Mobile Phone Users' Privacy [Online]. http://www.engr.mun.ca/~mhahmed/privacy/mobile_phone_privacy_report.pdf .
- Altarum Research Group (2007) Review of the personal health record (PHR) service provider market: privacy and security. https://www.cdt.org/healthprivacy/PHRs_Altarum_2007.pdf .
- Avancha, S., Baxi, A. and Kotz, D. (2012) Privacy in mobile technology for personal healthcare. ACM Computing Surveys (CSUR), 45 (1), 1-54.
- Checkland, P. and Poulter, J. (2006) Learning for action: a short definitive account of soft systems methodology and its use for practitioners, teachers and students. Wiley, Chichester.
- Dumortier, J. and Verhenneman, G. (2013) Chapter 2: Legal regulation of electronic health records: a comparative analysis of Europe and the US. In: George, C., Whitehouse, D. and Duquenoy, P. (ed) eHealth: legal, ethical and governance challenges. Springer. Berlin.
- Li, J. (2013). Electronic Personal Health Records and the Question of Privacy. IEEE Computer Society, 99, 1.
- Lindeman, D. (2011) mHealth technologies: applications to benefit older adults. [Centre for Technology and Aging]. http://phi.org/uploads/application/files/ghcah59qtuhe4iqhf3h7kp12v7q8xv15quh6u99569k1zuz ce7.pdf .

Bibliography

- Martino, L. and Ahuja, S. (2010) Privacy Policies of Personal Health Records: An evaluation of their effectiveness in protecting patient information. *Proceedings of the 1st ACM International Health Informatics Symposium*. ACM, 2010.
- Pritts, J.L. (2008) The importance and value of protecting the privacy of health information: the roles of the hipaa privacy rule and the common rule in health research. http://www.iom.edu/~/media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.ashx.
- PwC (2012) Emerging mHealth: paths for growth. PwC Health Research Institute. http://www.pwc.com/en_GX/gx/healthcare/mhealth/assets/pwc-emergingmhealth-exec-summary.pdf
- Steele, R., Min, K., and Lo, A. (2012) Personal health record architectures: technology infrastructure implications and dependencies. Journal of the American Society for Information Science and Technology, 63 (6), 1079-1091.

Thank you