Personal Health Data –Privacy Policy Harmonization and Global Enforcement

Pekka Ruotsalainen[a,1], Jaime Delgado[b], Bernd Blobel[c], Paulette Lacroix[d], Yukio Kurihara[e], Peter Pharow[f], Katerina Stechova[g], Tony Sahama[h]

[a] *University of Tampere, School for Information Science, Tampere, Finland*
[b] *Universitat Politecnica De Catalunya, Barcelona, Spain*
[c] *University of Regensburg, Medical Faculty, Germany*
[d] *PC Lacroix Consulting Inc, North Vancouver, BC, Canada*
[e] *Kochi University, Health Informatics Division, Japan*
[f] *Fraunhofer Institute for Digital Media Technology IDMT, Ilmenau, Germany*
[g] *University Hospital Motol, Prague, Czech Republic*
[h] *Queensland University of Technology, Brisbane, Australia*

Abstract. This workshop is jointly organized by EFMI Working Groups Security, Safety and Ethics and Personal Portable Devices in cooperation with IMIA Working Group "Security in Health Information Systems". In contemporary healthcare and personal health management the collection and use of personal health information takes place in different contexts and jurisdictions. Global use of health data is also expanding. The approach taken by different experts, health service providers, data subjects and secondary users in understanding privacy and the privacy expectations others may have is strongly context dependent. To make eHealth, global healthcare, mHealth and personal health management successful and to enable fair secondary use of personal health data, it is necessary to find a practical and functional balance between privacy expectations of stakeholder groups. The workshop will highlight these privacy concerns by presenting different cases and approaches. Workshop participants will analyse stakeholder privacy expectations that take place in different real-life contexts such as portable health devices and personal health records, and develop a mechanism to balance them in such a way that global protection of health data and its meaningful use is realized simultaneously. Based on the results of the workshop, initial requirements for a global healthcare information certification framework will be developed.

Keywords. Health data, privacy protection, context, privacy expectation, policy harmonization, enforcement, certification.

1. Introduction

This joint workshop will establish EFMI and IMA's second security-related collaborative event by EFMI "Security, Safety and Ethics" and "Personal Portable Devices" Working Groups and the IMIA "Security in Health Information Systems" Working Group

Currently, healthcare services and the collection and processing of personal health data increasingly take place across organisational, geographical and regulatory borders (e.g. in cross-organisational eHealth, in mHealth and pHealth). Personal Health

[1] Corresponding Author.

Information (PHI) is collected, used and disclosed in many contexts by different healthcare and non-healthcare groups and for various purposes. In spite of the existence of global privacy guidelines such as Fair Information Practice Principles and the IMIA Code of Ethics for Health Information Professionals [1,2] it is common that stakeholders such as the subject of care (a person or patient) medical practitioners, researchers, pharmaceutical industry representatives and statisticians all have their own expectations on how and for what purposes PHI should be used, and this may differ greatly from the expectations of the data subject – the individual patient, resident or client. Furthermore, each of these stakeholders has a different understanding and opinion concerning the level of privacy protection that information requires. For example, a medical practitioner may inappropriately share PHI with others outside of the circle of care, based on a belief that too much privacy and limited access to the PHI could put the patients' health at risk. Researchers may posit that less restricted access to PHI and Electronic Health Records would help them to better comprehend origin and functionalities of diseases, enabling improved medications and treatments. The data subject (e.g. the patient or person) may themselves elect to limit primary and secondary use of his or her PHI, expressing privacy concerns and lack of information autonomy or trust [3].

The concept of privacy itself is complex, dynamic and related to sensitivity of information, context where it is used, purpose of use and trust [4]. Furthermore, privacy has personal, regulatory and social dimensions [5]. Context can be understood as a set of information characterising the situation of an entity (e.g. physical environment, state of people, internal tasks, and computational and physical objects) [6]. Contemporary healthcare and the use of personal health services increasingly takes place in many contexts. A prerequisite for fair and meaningful use of PHI is the need for determining in each context an appropriate level of privacy that satisfies all stakeholder requirements. In other words, it is necessary to find a mechanism that balances different privacy expectations.

From a privacy management point of view, contemporary health services such as mobile health and personal health record systems, which use as backbone unsecure networks such as the Internet and mobile networks, are extremely challenging. From a privacy protection perspective, cross-organisational and global healthcare urgently needs context-aware privacy protecting that takes into account stakeholders' privacy expectations.

This is especially true in the provision of cross-jurisdictional eHealth services where context-aware privacy protection is demanding at best as many contextual features cannot be predicted or planned for. International privacy legislation is variable, and in some areas non-existent. PHI is highly sensitive data that has value not only for research and analysis, but more recently is sought after for identity theft and other fraudulent uses [7]. A proposed solution to balancing the global privacy rights of the individual with the access, use and disclosure of PHI is the development of a healthcare information certification for service providers and healthcare entities. A starting point for those requirements is the understanding of context-aware privacy expectations of each stakeholder and a mechanism for balancing the different interests.

2. Aim of the discussion

In the first part of the workshop participants will identify stakeholders' privacy expectations in different contexts using generic context-aware privacy models [4,8]. Differences and similarities will be contrasted to determine how privacy and its dimension are understood by each of the stakeholders and how PHI is used in specific situations. These findings will be analysed from the various stakeholder points of view (e.g. healthcare service provider, patient, person managing own health, secondary users such as statisticians, researchers, pharmaceutical industry representatives, and the healthcare entity itself) [9].

The origin and features of conflicting privacy expectations and privacy unease related to these different contexts will be discussed. Privacy concerns induced by ICT-technology, such as mobile devices, wearable device/sensors, communication networks, personal health devices, records, cloud services, etc. will analysed collectively with stakeholders' privacy expectations. Based on the outcome of this discussion, emerging themes will inform areas where privacy expectations can lead to potential conflict and where a mechanism for balancing different interests would be most valuable. Finally, balancing methods and the enforcement of privacy principles (policies) under changing contexts will be discussed.

In the second half of the workshop, the participants will focus on the challenges of protecting PHI in a global context, given the context-aware privacy expectations of various stakeholders. The proceedings will be led by international experts who will introduce Ethical, Legal, Technical and Business Model-based challenges in the global protection of PHI. The concept of an international healthcare certification framework for both service providers and healthcare organizations will be introduced and explored in relation to privacy expectations, core requirements of a certification program, qualified entities to certify healthcare providers, implications for global health tourism and enforcement requisites.

The final discussion will combine the findings on contextual privacy expectations and balancing mechanism with a global privacy protection certification framework for PHI. Results of this joint workshop will assist in the foundational development of a global initiative to balance privacy expectations for use of PHI between all stakeholders.

3. Workshop Speakers

The first part the workshop is jointly organised by EFMI WG SSE and WG PPD. The second half of the workshop is the 2nd Joint WS of EFMI WG SSE and IMIA WG SiHiS, and will take place under the lead of IMIA SiHiS WG.

- Pekka Ruotsalainen, Adjunct Professor, Research Professor Emeritus, University of Tampere, Finland, vice-chair and acting Chair EFMI WG SSE, Co-Chair and acting chair IMIA SiHiS.
- Jaime Delgado, Full Professor, Universitat Politècnica de Catalunya, Barcelona, Spain, Vice-Chair EFMI WG SSE.

- Bernd Blobel, Professor, former Chair of EFMI WGs SSE and EHR, former Vice-Chair of IMIA WG SiHiS, Medical Faculty, University of Regensburg, Germany
- Paulette Lacroix, HBScN, MPH, CMC, CIPP/C, CIPP/US, PC Lacroix Consulting Inc., North Vancouver, BC, Canada
- Yukio Kurihara, Professor, Kochi University, Kochi, Japan
- Peter Pharow, Vice Chair EFMI WG PDD PPD, Fraunhofer Institute for Digital Media Technology IDMT, Ilmenau, Germany
- Katerina Stechova, MD, associate professor, University Hospital Motol, Prague, Czech Republic
- Tony Sahama, Senior Lecture, Dr, Science and Engineering Faculty, Electrical Engineering, Computer Science, Queensland University of Technology, Brisbane, Australia

4. Contribution from each speaker

The workshop has been structured to follow the previously successful model applied in the first joint SSE/SiHiS WS (Istanbul 2014) that both informs the participants and allows for their successful participation. A short introduction will outline the themes and expected outcomes. In the first part of the workshop (led by EFMI WG SSE) international experts will analyse contextual features of privacy expectations from different stakeholder viewpoints. After short presentations the experts and WS participants together will discuss ways to balance different privacy expectations.

In the second half of the workshop (led by IMIA WG SiHiS), international experts will present an ethical code that supports global protection of PHI and introduction of a healthcare certification program model. After these presentations, the participants and experts will discuss the findings from the first session on context-awareness privacy expectations and how they should be taken into account in the development of a framework for certification of privacy protection globally. Finally, a summary of the results from both sessions will be presented together with a suggested way forward.

- Professor Pekka Ruotsalainen, Context-aware Privacy Models and Privacy Dimensions, Session 1 chair. Discussion and Conclusions.
- Professor Bernd Blobel, Indirect and Direct Health Data Context Specification and its Harmonization (part 1). New Challenges and Solutions for Privilege Management and Access Control in Ubiquitous Health (part 2)
- Professor Jaime Delgado, Levels of Privacy Protection and their Impact in the Medical Practice and Study.
- Katerina Stechova, Challenges and Conflicts between the Meaningful Use of Health Data and Patients' Privacy Expectations.
- Peter Pharow, eHealth and its Context Dependent Privacy Issues for Applying Personal Portable Devices.
- Paulette Lacroix, Challenges in the Global Protection of PHI. Advancing Context Appropriate Privacy Protections. Session 2 chair.
- Professor Yukio Kurihara, Japanese Scheme for Protection of PHI and its Necessary Improvements for Extending Secondary use of PHI.

- DrTony Sahama, The Information Accountability Model for Global eHealth.

5. Expected results

This workshop will identify stakeholder needs, concerns and privacy conflicts regarding PHI under changing contexts, and it will draft a context-specific privacy balancing mechanism for managing conflicts in the use of PHI and a global privacy protection certification framework for PHI. Outcomes of the workshop will be published to initiate wider discussion.

6. Time required

Due to the proposed structure of presentation to include debate and concluding discussions, we kindly request the SPC to assign two time slots for this workshop. This proposed approach was highly successful at the previous joint EFMI/IMIA workshop at MIE2014 in Istanbul.

References

[1] U.S. Department of Health, The Code of Fair Information Privacy Principles, U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973).

[2] IMIA, IMIA Code of Ethics for Health Information Professionals, http://www.imia medinfo.org/new2/node/39.

[3] Caine K, Hanania R: Patients want granular privacy control over health information in electronic medical records. Journal of the American Medical Informatics Association 2013, 20(1):7-15.

[4] Nissenbaum H: Privacy in Context: Technology, Policy and the Integrity of Social Life. Stanford, California: Stanford University Press; 2010.

[5] Westin A F, Social and Political Dimensions of Privacy, Journal of Social Issues, Vol. 59, No2 2003, DOI: 10.1111/1540-4560.00072.

[6] Dustdar S, Baldauf M, Rosenberg S, A survey on context-aware systems, Int. J. Ad Hoc and Ubiquitous Computing, Vol. 2, No. 4, 2007.

[7] Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 7, 2015 http://www.ponemon.org/news-2/66.

[8] Lederer S, Deay AK, Mankoff J. A conceptual model and metaphor of everyday privacy in ubiquitous computing environments UC Berkeley College of Engineering Technical Reports. Berkeley, CA: Computer Science Division, University of California; 2002 Jun. URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2002/CSD-02-1188.

[9] Ruotsalainen P, Blobel B, Seppälä A, Nykänen P. Trust Information-Based Privacy Architecture for Ubiquitous Health JMIR Mhealth Uhealth 2013;1(2):e23), doi:10.2196/mhealth.2731.