MEDINFO 2017: Precision Healthcare through Informatics
A.V. Gundlapalli et al. (Eds.)

doi:10.3233/978-1-61499-830-3-202

Trust Model for Protection of Personal Health Data in a Global Environment

Pekka Ruotsalainen[a], Bernd Blobel[b]

[a] *School for Information Science, University of Tampere, Finland*
[b] *Medical Faculty University of Regensburg, Germany*

Abstract

Successful health care, eHealth, digital health, and personal health systems increasingly take place in cross-jurisdictional, dynamic and risk-encumbered information space. They require rich amount of personal health information (PHI). Trust is and will be the cornerstone and prerequisite for successful health services. In global environments, trust cannot be expected as granted. In this paper, health service in the global environment is perceived as a meta-system, and a trust management model is developed to support it. The predefined trusting belief currently used in health care is not transferable to global environments. In the authors' model, the level of trust is dynamically calculated from measurable attributes. These attributes describe trust features of the service provider and its environment. The calculated trust value or profile can be used in defining the risk service user has to accept when disclosing PHI, and in definition of additional privacy and security safeguards before disclosing PHI and/or using services.

Keywords:
Trust; Health Records, Personal ; Privacy

Introduction

Starting from Hippocratic time, trust has been one of the main cornerstones in successful healthcare. Until now, trust and distrust have not been big questions in today's health care. Instead, it is expected that both health care services and their information systems occur in a controlled environment where ethical codes and laws guarantee fair and trustworthy information processing. It is also expected that patients intrinsically trust the health care service provider, and believe that information systems and networks that communicate, process, and store patients' personal health information (PHI) are trustworthy. In other words it is argued that predefined organizational trust is sufficient, and security based access controls guarantee privacy [1].

However, health care in general is in transition. Health care services and information systems are increasingly provided cross-organizationally, across boundaries, and cross jurisdictionally. New services models such as digital health, personal health, health eco-systems, and ubiquitous health take place in global information networks. They are built on using modern information and communication technology (ICT), global communication networks, and applications as service. This implies that service providers, customers, patients, the PHI and applications can operate in different contexts and jurisdictions. Furthermore, the PHI is increasingly collected, used, communicated and stored in environments not regulated by health care or privacy laws, global guidelines, codes of conducts; and fair information processing rules are implemented just poorly or even worse, not at all. It is also common that service provider, service user (a person or patient), medical practitioners, secondary users of PHI and health software developers can all have their own notion of how PHI should and can be used and protected. This may basically differ from the expectations of the data subject and his or her local regulations.

From the standpoint of privacy and trust, the modern global and distributed health service environment is challenging. First, in the context of cross-jurisdictional e-health and personal health services, contextual trust and privacy features cannot be predicted or measured in advance. Secondly, the network itself is unsecure, and the data collector or customer has few or no tools to measure the level of trust. Furthermore, he/she has limited or no power to enforce informed privacy and security decisions concerning the trustworthiness of services and control how, by whom and for what purposes PHI is collected and processed [2].

It is widely accepted that trust and privacy are key enablers for global health care and the use of personal health services. Using the self-regulation principle, industry has developed trust, security and privacy rules for eCommerce. Unfortunately, those rules are most of all developed to support industry's own business needs, expecting that customers blindly trust on the service provider and accept rules as they are (i.e. take-or-leave principle). Yuan and Ruotsalainen et al. have mentioned that increasingly modern health care and ubiquitous health services are dynamic and take place in unsecure and uncertain environment where no predefined trust cannot be expected [2, 3]. This indicates that current rules used by eCommerce cannot be moved to health services as such.

The authors state that health information is highly sensitive requiring special protection. To enable trustworthiness of global health care and the use of personal health services, there is an urgent need for practical and easy-to-use solutions for trust measurement, trust creation and management. Without such prerequisites, it can be dangerous for a service provider to disclose PHI, and for a customer (persons and patients) to use offered services. In global environments, it is also necessary that customers using services and service providers disclosing the PHI can make rational and information based choices concerning additional safeguards needed, in advance.

This paper is based on the following assumptions: Privacy and trust are interrelated concepts in a way that less trust requires more privacy protection. Trust is situational and context-

dependent. Knowing the trust level of a health service provider enables the service user (patient, person or organization) to make rational choices concerning to what extent it has the willingness to use services, and what amount of PHI it is ready to disclose at certain level of trustworthiness. In global environments, trust features expressed in the form of trust value or trust profile enable the service user to define necessary safeguards before starting the use of services.

Previous research

Trust is a multifaceted, context-dependent concept, and a term with many meanings. There is no globally agreed definition for it. Widely used trust models are trusting belief, organization/institutional trust, dispositional trust, recommended trust, direct trust, and computational trust [4]. In the context of global health services, trust can be seen as a process of practical reasoning that leads to the decision to interact with somebody [5]. Institution-based trust deals with structures (e.g. legal protections) that make an environment trustworthy. Institutional trust is the belief that needed structural conditions are present [6]. System trust represents the extent to which a customer believes that the proper structures are in place, i.e. that reasonable safeguards are in place to reduce risk. These safeguards may be represented in form of regulations, guarantees, or stabilizing intermediaries [7].

Ruotsalainen et al. have noted that in networked and ubiquitous health service systems dispositional trust, recommended trust, and direct trust are not much stronger than belief, and organizational trust is static [2]. Because the use of global health services is increasingly dynamic, it requires the possibility to make online trust decisions.

Trust models are often based on use of a pure numerical approach. The mechanisms used to calculate trust values range from simple aggregation of values to the use of probability theory, fuzzy logic, or the use of entropy [8]. The number of past experiences, observation interaction, and recording are also widely used [5].

According to Saadi et al., previously discussed "classical" trust approaches that cannot be adapted to networked and ubiquitous environments such as cross-jurisdictional healthcare and personal health systems where the unpredictability and unreliability of service location, contextual features, regulation and rules make mechanisms inappropriate [9].Viljanen et al. have defined a trust formulation process using trustors contextual attributes and actions, information attributes, social and ethical attributes and third party information (e.g. certificates or recommendations)[10].

Trust models are developed especially for multi-agent systems, Mobile Area Networks (MANET), and open dynamic and ubiquitous environments [5,11,12]. In MANETs, trust is typically evaluated using transaction history of past interactions and transactions and others recommendations. Another approach is the use of trusted third parties and certificates [13]. Hereby, calculated trust values are deployed as estimates of the service provider's trustworthiness [14].

Ruotsalainen et al. have proposed the following attributes for trust calculation in pervasive health: trustor's environmental factors and contextual features, ICT systems properties, privacy policy, predictability, transparency and openness, and system's regulatory compliance [2].

Methods

In this paper, the collection and use of the PHI in global environment is perceived as a meta-system characterized by its structure, functions, behaviour, and relevant stakeholders. Using system modelling methods, system analysis and system engineering techniques, a conceptual trust management model for the protection of PHI in global environment is developed.

Based on a careful analysis of findings and proposals from research published in journals and conference proceedings, measurable trust attributes are identified. Attributes are aimed for the evaluation of the level of trust of different kind of health providers and secondary users of the PHI in existing in global environment.

Results

Because the global health service environment forms a meta-system, trust should be created between its actors. According Saadi, Sabater-Mir and Zheng [2, 8, 9, 14], the authors state that belief and recommendation based trust solutions are too weak. Instead, dynamic system trust that is based on service provider's real life measurable features is the most promising approach.

Trust Management Model

Because the use of PHI takes place in different contexts, contextual trust approach is needed. According to Jøsang et al., contextual trust describes the extent the data subject can expect that necessary services and institutions are in place in order to support trustworthy communication; and trust implies a decision [15]. As discussed earlier, belief as well as dispositional and recommended trust approaches cannot be used in dynamic, distributed environments, and meaningful trust decisions are impossible without reliable information. Therefore, the approach of calculated contextual system trust that is based on measured features of service providers is selected for the model. Thereby, policies can be used to define what is permitted or prohibited, and what security and privacy obligations the service provider must perform in advance.

The proposed model for trust management in global health services is shown in Figure 1. The model is focused on the processing of PHI in different contexts and environments. The model is developed and presented using UML.

In the model, service providers can be either regulated or nonregulated health service providers, or other entities processing PHI (e.g. secondary users). Non-regulated service providers include institutions beyond regulated healthcare establishments such as personal health systems, personal health and ubiquitous-health services. From a data processing perspective, service providers are represented by different instances such as data creator, data controller and data processors [16]. The data controller manages, stores, and discloses personal health information to data processors. Data processors use disclosed health data on behalf of data controllers [16].

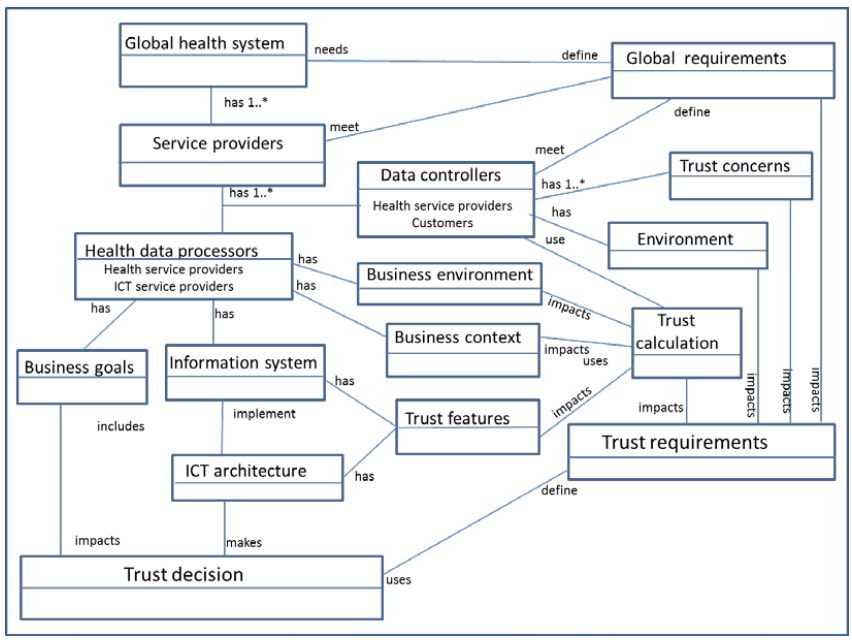

Figure 1 - A conceptual model for the trust management in global health

The data controller can be a health care provider/providing organization or the data subject (a person or patient). The data processor is any entity deploying received PHI during its service process. The data processor has own business goals such as offering health service or using PHI for research. In global health settings, the data controller often has no predefined trust to the service provider to whom PHI is disclosed to. Instead it has trust concerns.

The data processor deploys an information system with an appropriate ICT architecture (the concept of a system covers both components and processes, i.e. structure and behaviour of that system). One component of the ICT system is the trust decision application. It is typically an Artificial Intelligence solution.

The environment includes national and international regulations, laws and norms guiding the processing of PHI, e.g., security and privacy regulations.

The business environment is a combination of external and internal factors such as organizational rules and constraints in the framework of national and international regulations. The business context of the data processor in the system in question includes expectations of other parties involved such as the data controller/customer, but also process-specific constraints, technologies, etc.

Global requirements include ethical principles and codes of conduct, international Golden Rules (e.g. Fair Information Practice Principles, OECD principles), standards and international certification requirements (e.g. possible future global privacy regulations for health services).

Because trust and privacy are interrelated in such a way that lower trust requires more privacy safeguards, both trust requirements (e.g. audit-log for transparency, policy based access control as properties of the ICT system, standards for reliability) and privacy requirements such as anonymization and denying the post-release of the PHI have to be managed.

Trust creation provided by the data controller requires that the level of trust of the data processor can be defined, formalized and communicated. In the model, the Trust calculator service (e.g. an agent application) collects necessary information for the calculation of trust level or trust profile of the service provider and communicates this information.

The Trust Requirements service uses information received from the Trust calculator, Trust concerns, Global requirements and service providers Trust features to define rules (policies) the service provider offering health service should follow. System requirements such as audit-log, policy based PHI management, notification, and privacy requirements such as anonymization and denying the post-release of the PHI are expressed in the form of computer understandable policies as defined in ISO 22600. In the proposed model, each service provider is first authenticated and then assigned to a trust value or trust profile. Trust and privacy requirements associated to a service provider are processed by its trust decision application.

The presented model is suitable for both static and dynamic online situations in global environment. For example, the Trust calculator can be a Certification Authority (a Trust CA) that generates trust certificates for service providers, and compares them against data controller's certificate.

Trust attributes

In the developed model, trust attributes are needed and used to measure the amount of trust. Researchers have suggested more than 40 different trust attributes [6, 14, 17, 18, 19, 20] (Table 1). Seppanen et al. have defined benevolence, competence, fairness, honesty, moral integrity, motivation, predictability, and reputation as most common trust attributes [21].

The challenge with most of trust attributes shown in Table 1 is that they are difficult to conceptualize and to measure. Therefore, it is also difficult in global environment to generate common understanding for attributes. For overcoming that problem, the concepts should be represented explicitly using ontology representation tools.

Table 1 - Common trust attributes

Ability	Competence	Likeability	Responsibility
Authenticity	Data quality	Moral integrity	Receptivity
Benevolence	Fairness	Motivation	Reciprocity
Certificates	Frankness	Recommendation	Risk assessment
Credibility of promises	Judgment	Openness	Security
Confidence	Honesty	Past interactions	System reliability
Consistency	Habitualization	Privacy policy fulfilment	Togetherness
Discreteness	Integrity	Reputation	Transparency
Integrity	Intention	Predictability	Tracking
Confidentiality	Institualization		Transactions
	Legal requirements		Trustee's promises

To make attributes acceptable and implementable at global level, the authors propose the following set of attributes for the calculation of trust when health services are used in global environment:

- Ability and willingness
- Integrity
- Openness and transparency
- Properties if service providers manage the ICT system
- Predictability of promises
- Reliability of service provider's promises
- Service provider's environmental factors and contextual features
- Service provider's regulatory compliancy
- Willingness to follow rules (policies) the data processor define

Attributes presented above form a minimum set of attributes that can be measured in real life situations.

Ability can be calculated from direct measurement and/or from the systems' past history [2]. Integrity addresses that the service provider accepts rules and meets its promises [18]. This can be measured using systems' history and other's witnesses. Openness and transparency means that service provider's security and privacy policies, audit trail, standards and laws used, evaluation and risk assessment documents are openly available, and the security and privacy breaches will be notified to the data controller. Properties of the service providers' ICT systems can either be identified from evaluation or assessment reports, with the help of system documents and features expressed in contract documents, or from trust certificates. Predictability concerning service provider's promises can be measured using systems history or continuous monitoring. Service provider's contextual and environmental features can be resolved by available information concerning service provider's location and business goals. Regulatory compliance can be measured using conformance assessment and the regulatory compliance documents. Willingness to follow rules (policies) the data controller has defined can be measured either by direct measurements or by monitoring.

In the model, trust value can be expressed using the scale proposed by Liu [22]: Compromised or malicious, unable to determine trust-level, low trust level, medium, fairly high trust level, and extremely high trust level. For more detailed trust creation, the data controller can use rich trust profiles received from the Trust calculator [2]. Based on calculated trust values, the data subject can define service provider specific data processing policies for all organizations and persons participating in the service provision chain, and for all secondary users [2].

Discussion

In this paper, the authors proposed a novel trust formulation and management model for health care and health information systems operating in the global information space. The model enables the data controller to disclose PHI, and the customer to use networked health services, by creating and managing contextual trust across geographical, cultural and jurisdictional borders. The authors have also proposed nine measurable trust attributes which the data controller can use in defining additional service provider specific privacy requirements.

The proposed model is flexible. For example, it accepts the use of certificates. Unfortunately, a typical certificate represents only a digital identity of the users, and is static [9]. Therefore, a trust certificate that can be used for the evaluation of trust level requires much richer information such as the trust profile.

In the model presented, the data controller (data subject or organization controlling the use of PHI) can make informed policy decisions by balancing service benefits expected and own privacy needs against trust level of the data processor. A strength of this model is that it enables the calculation of trust level/profile in cases where only incomplete information of data processor's trust features is available. The latter situation generates low trust value. In this way, the proposed solution is proactive and stresses the data processor to support openness and transparence. Challenges include the development of trust calculation services and the global agreements on trust attributes. This might require political and legal actions at global level. It is also necessary to test the feasibility of proposed attributes, and standardize their presentation and meaning. In the future, it is also necessary to demonstrate that the proposed solution is technically valid, reliable and easy to use. Globally, the biggest challenge is to make the principle of direct measurement based on calculated trust accepted by health industry, healthcare professionals and organizations. International political, legal, regulatory and organizational actions are needed to make this true.

Conclusion

The authors have developed a conceptual model for trust management in global, cross-organizational and cross-jurisdictional health service environment. The model enables the data controller (a person or organization) to evaluate the level of trustworthiness of the data processor before starting to use services or to disclose PHI. Both regulated healthcare and nonregulated health services models are supported. For trust evaluation/calculation, a set of practical and measurable trust attributes is proposed.

In the model, trust level is expressed as trust value or trust vector. The model enables the data controller to define for the service provider minimum privacy and security safeguards required to be qualified trusted.

References

[1] Ruotsalainen P, Blobel B, Seppälä A, Sorvari H, Nykänen P, A Conceptual Framework and Principles for Trusted Pervasive Health, J Med Internet Res 2012;14(2):e52 doi:10.2196/jmir.1972.

[2] Ruotsalainen P S, 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.

[3] Yuan W, Guan D, Lee S, Lee Y-K The Role of Trust in Ubiquitous Health Care, 9th International Conference on e-Health Networking, Application and Services, IEEE Xplore July 2007 DOI: 10.1109/HEALTH.2007.381660.

[4] Sabater J, Sierra C: Review on computational trust and reputation models, Artif Intell Rev (2005) 24: 33. doi:10.1007/s10462-004-0041-5.

[5] Pinyol I, Sabater-Mir J, Computational trust and reputation models for open multi-agent systems: a review, Artif Intell Rev (2013) 40:1–25, DOI 10.1007/s10462-011-9277-z.

[6] McKnigth DHC, Choudhury V, Kacmar C, Developing and Validating Trust Measures for e-Commerce: An Integrative Typology, Information Systems Research, Volume 13 Issue 3, September 2002 Pages 334-35, doi:10.1287/isre.13.3.334.8.

[7] Gray E, O'Connell P, Jensen C, Weber S, Seigneur JM, Yong, Towards a Framework for Assessing Trust-Based Ad mission Control in Collaborative Ad Hoc Applications,2002 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.4803&rep=rep1&typ.

[8] Sabater-Mir J, Towards the next generation of computational trust and reputation models**,** Proceedings of the Third International Conference on Modeling Decisions for Artificial Intelligence (MDAI'06), 19-21, ISBN:3-540-32780-0 978-3-540-32780-6, doi>10.1007/11681960_4.

[9] Saadi R, Pierson JM, Brunie L. (Dis)trust Certification Model for Large Access in a Pervasive Environment, International Journal of Pervasive Computing and Communications, (2005) Vol. 1 Is: 4, pp.289 - 299 ISSN: 1742-7371.

[10] Viljanen, Towards an Ontology of Trust, In Katsikas S, Lopez I and Pernul G (Eds.) Trust, Privacy and Security in Digital Business, Proceedings of the 2nd International Conference TrustBus 2005, Copenhagen, Denmark ,August 22-26 2005, LNCS 3592 Springer.

[11] Matt PA, Morge M, Toni F, Combining statistics and arguments to compute trust, AAMAS '10 Proceedings of the 9th International Conference on Autonomous Agents and Multi-agent Systems: volume 1 - Volume 1 Pages 209-216, 2010, ISBN: 978-0-9826571-1-9.

[12] Velloso P B, Laufer RP, Cunha D, Duarte O, Pujolle G, Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model I, EEE transactions on network and service management, VOL. 7, NO. 3, September 2010.

[13] Omar M, Challal Y, Bouabdallah A Certification-based trust models in mobile ad hoc networks: A survey and taxonomy, Journal of Network and Computer Applications October 30, 2011, https://hal.archives-ouvertes.fr/hal-0064449,2011.

[14] Zheng Y, Holtmanns S, "Trust Modeling and Management: from Social Trust to Digital Trust", book chapter of Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, IGI Global, 2007.

[15] Josang A, Ismail R, Boyd V: A Survey of Trust and Reputation Systems for Online Service Provision, Journal Decision Support Systems, Volume 43 Issue 2, March, 2007, Pages 618-644.

[16] EU Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX: 31995L0046:en:HTML

[17] Becerra G, Heard J Kremer R, Denziger J, Trust Attributes, Methods, and Uses, In Proceedings of the Workshop on Trust in Agent Societies, AAMAS-2007 Honolulu Hawaii USA; May 2007, 1-6, https://www.researchgate.net/publication/ 28814176_Trust_attributes_methods_and_uses.

[18] Hussin Ab RC, Macaulay L, Keeling K. The importance ranking of trust attributes in e-commerce Website. 2007 Presented at: Proceedings of the 11th Pacific-Asia Conference on Information Systems; Jul 3-7, 2007; Auckland, New Zealand URL: http://www.pacis-net.org/file/2007/1247.pdf.

[19] Kim, Dan J. Ferrin, Donald L. RAO, H. Raghav. A Trust-Based Consumer Decision Model in Electronic Commerce: The Role of Trust, Risk, and Their Antecedents. (2008). Decision Support Systems. 44, (2), 544-564. Research Collection Lee Kong Chian School of Business.

[20] Mayer RC, James JH, Schoorman FD, An integrative model of organizational trust, Academy of Management Review 1995, Vol. 20. No. 3, 709-734.

[21] Seppanen R, Blomqvist K, Sundqvist S, Measuring inter-organizational trust – a critical review of the empirical research in 1990-2003, Industrial Marketing Management 26(2007), 249-265.

[22] Liu Z, Robert A W J, Thompson R A,A Dynamic Trust Model for Mobile for Mobile Ad-Hoc Networks, Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04) 0-7695-2118-5/04, 2004 IEEE.

Address for correspondence

Pekka Ruotsalainen, Adjunct Profesor, Research Professor emeritus, University of Tampere, Finland,Chair IMIA WG SiHiS. E-mail: pekka.ruotsalainen@uta.fi.