*Informatics, Management and Technology in Healthcare*
*J. Mantas and A. Hasman (Eds.)*
*IOS Press, 2013*


*doi:10.3233/978-1-61499-276-9-129*

# A conceptual security framework for personal health records (PHRs)

Mikaela POULYMENOPOULOU[1], Despina PAPAKONSTANTINOU, Flora MALAMATENIOU, Andriana PRENTZA and George VASSILACOPOULOS
*Department of Digital Systems, University of Piraeus, Piraeus, Greece*

**Abstract.** Electronic personal health record (PHR) is a citizen-centric information tool that allows citizens to control their personal information. However, an ideal PHR should also allow citizens to connect with their formal and informal caregivers (e.g. a family member, a caregiver) and together manage citizen health and social information. This introduces specific challenges in terms of security since multiple parties make entries and require access to PHR data. Since citizens are typically non-security and non-domain experts is considered impossible to control all this information. To this end, this paper presents a conceptual security framework for the employment of an attribute-based PHR access control policy that is continually updated according to providers' local security policies and individual professionals and citizen sharing preferences.

**Keywords.** Personal health record, security, attribute-based authorization

## Introduction

Lately, citizen-centered care has been proposed as a solution for integrating citizens disparate health and social care information and the Personal Health Record (PHR) is a citizen-centric informational tool that could provide healthcare consumers access to health information and allow citizens to control their personal information [1,2]. However, currently citizens seem unable or not willing to 'unify' their disparate care experiences in a PHR and providers usage of PHRs remains low mainly due to their concerns for the reliability of citizen generated data that might even be altered or forged [2,3]. An ideal PHR system should correspond to an integrated care ecosystem where citizens are connected with their formal and informal caregivers consisting citizen network of care, who are the primary source of citizen health and social care information and legitimate users of PHR, and together manage citizen information.

With the recent advancement of cloud computing, PHRs are typically cloud-based that ensures availability and improved service quality while reduces the capital and operational expenditures. Those PHRs store and process very sensitive information and multiple parties (providers, family) require access to this information and therefore the complexity to manage data security and privacy increases. In most, public cloud-based PHRs, the citizen is only empowered to control his health information [2,3]. However a general problem is how the citizen, considered a non-security and non-domain expert can declare access control policies on information that might even can't understand. On the contrary, a security model where not only the citizen but also individual

[1] Corresponding Author. Mikaela Poulymenopoulou; e-mail address: mpouly@unipi.gr

professionals and providers authorized by the citizen control access to information entered by them might be more suitable for PHRs with multi party access.

In this paper, is defined the cloud-based PHR system as a set of services that integrate medical and social care information over time from the citizen and sites of care in a structure (clinical documents) that is readily accessible. The security requirements of such a PHR are presented and a conceptual security framework is proposed for the employment of an attribute-based access control policy which is a combination of the policies defined by the citizen, the individual professionals and providers of citizen network of care where each policy applies to the information added by the policy creator.

## 1. PHR security requirements

In the cloud-based PHR system is assumed that there exists a basic PHR security policy as determined by relevant regulations and ethical rules that is used to govern access to citizen records in the absence of explicitly specified preferences [3]. This policy is enhanced with access control rules created by the citizen and multiple PHR users authorized by citizen as illustrated in Figure 1.

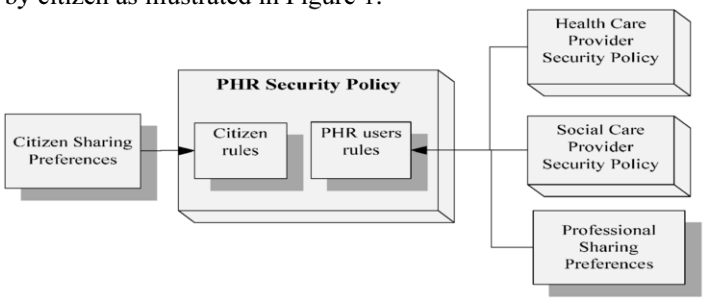


**Figure 1.** The PHR security policy of the cloud-based PHR

A subset of the basic access control requirements for the PHR model is:

- Citizen information is structured in the form of hierarchical XML data elements. Each element has an owner and falls under a category like medications, results etc.
- The citizen is the owner of the information added by him and non-professionals and controls it through the creation of access control rules.
- The citizen authorizes PHR users to add health and social information.
- The citizen can revoke authorization to PHR users at anytime.
- The individual professionals and providers are the owners of the information added by them and control it through the creation of access control rules.
- Citizens have read access to all citizen information existing in the PHR.
- The citizen consent is required for sharing citizen information among PHR users.
- Access control rules define positive permissions for PHR users.
- Access control rules are applied to specific users, user roles or groups and concern specific XML data elements owned by the rule creator or all XML elements under a category.

- The citizen can specify access control rules for exceptional situations (e.g. in case of emergency, for research purposes) where he/she will not be able to give consent.

## 2. Security framework

The proposed conceptual security framework follows service-oriented architecture (SOA) concepts and related standards and semantic technologies for interoperability purposes [1]. Hence, a PHR ontology is used for sharing among providers diverse systems the definitions of subject, resource and environment attributes used on attribute-based PHR policy. In particular, the ontology main classes are a) subject information (user roles and groups), b) medical information representing the categories of citizen XML documents, c) environmental information like temporal (e.g. time instances or intervals) and location information and d) situational context information (e.g. in an emergency). The ontology information is used by the administrator of each provider to create a mapping file among the roles, resources and environmental variables of the local access control rules to those defined in the ontology. The main components of this framework are: the access control base, the rule translator, the context manager where the PHR ontology exists and the web services. On the access control base is stored citizen and individual professionals defined security policies and the providers local security (enhanced) policies. A citizen access control rule can specify that information added by him/her under the category medical problems can be shared only with subjects certified as 'my general practitioner' and 'my family'. The rule translator translates the provider access control rules that are mostly role-based into attribute-based access control rules using the provider mapping file. The context manager infers the ontology each time new access control rules are created that might result to the creation of new access control rules. For example, a citizen access control rule might specify that in the situational context "in an emergency" the "Allergy" category should be available to professionals. The ontology is inferred and new rules are created specifying that all sub-elements under the "Allergy" section should be available to subjects "emergency physicians" or "ambulance personnel" being at the location "emergency room" or "ambulance". The web services communicate with all other components of the framework and are invoked by a) citizens to create 'write' access control rules, to revoke authorization from PHR users and to share citizen information owned by individual professionals/providers, b) citizens and individual professionals to create 'read' access control rules, c) individual professionals/providers to request consent to share citizen information with other PHR users and d) health/social care providers to create/update their access control policy on PHR.

## References

[1] J. Calvillo, I. Roman, L.M. Roa, Empowering citizens with access control mechanisms to their personal health resources, *International Journal of Medical Informatics* **82** (2013), 58-72.

[2] B. Pirtle, A. Chandra, An overview of consumers perceptions and acceptance as well as barriers and potential of electronic personal health records, *American Journal of Health Sciences* **2** (2011), 45-52.

[3] A. Mohan, D. Bauer, D. Blough, M. Ahamad, B. Bamba, R. Krishnan, L. Liu, D. Mashima and B. Palanisamy, A patient-centric, attribute-based , source-verifiable framework for health record sharing, In GIT CERCS Technical Report No. GIT-CERCS-09-11 (2009).