Smart Home Solutions for Healthcare: Privacy in Ubiquitous Computing Infrastructures

Marianthi Theoharidou, Nikos Tsalis, and Dimitris Gritzalis

Information Security and Critical Infrastructure Protection Research Laboratory
Dept. of Informatics, Athens University of Economics & Business
76 Patission Ave., Athens GR-10434, Greece
{mtheohar, ntsalis, dgrit}@aueb.gr

1. Introduction

Healthcare Information Technology (IT) enables access to advanced healthcare services for patients and medical staff. Smart homes (or places) enable patient self-treatment and monitoring by using *simple devices,* which provide standardized outputs for specific physiological conditions, *intelligent applications or software* capable of analyzing and processing body signals, *sensor integrated smart devices*, *wearable sensors* and other devices exclusively manufactured for the purpose of body signal monitoring/processing (Athavale, 2011). Whether at home or traditional settings (physician's office, hospital), healthcare IT infrastructures process sensitive patient health information and, thus, face several information security and privacy threats. Such threats, as well as their corresponding impact, have been presented in the past (Gritzalis, 1998) (see Table 1).

Smart homes fall into the pervasive computing paradigm. They utilize components (e.g. sensors), which may be invisible and transparent to the user. Their constantly increasing storage and communication capabilities coupled with their small size enable collection, processing, and potential disclosure of Personal Health Information (PHI), thus posing significant privacy risks (Dritsas et al., 2006). A comprehensive view of privacy challenges is depicted in a 2011 study on "Patient Privacy and Data Security" (see Figure 1). While smart homes are novel, security in healthcare is a studied issue. Available solutions focus in specific security attributes. For example, (Gritzalis and Lambrinoudakis, 2004) propose an architecture that preserves authentication and authorization in web-based distributed systems. Such architecture includes a role-based access scheme and an intelligent security agent, which can be applied in healthcare environments. (Lekkas and Gritzalis, 2006) cover the authenticity requirement for Electronic Health Records (EHR) in a long-term basis. Another approach (Gritzalis, 1997) focuses on the issue of protecting Health Information Systems (HIS) by proposing a methodology and a decision-support roadmap for the development of the security profile of a specific information system. Relevant standards regarding healthcare are also reviewed by (Gritzalis, 1998) through the use of a framework that identifies existing gaps and inconsistencies.

Security Concern/ Threat	Impact
Information Disclosure (Loss of Confidentiality)	Patient embarrassment; Loss of trust; Legal consequences; Loss of reputation.
Withholding Information or Services (Loss of Availability)	Poor quality of services; Insufficient patient treatment; Legal claims; Financial impact.
Modification of Information (Loss of Integrity)	Insufficient or inappropriate patient treatment; Poor management; Financial loss.
Repudiation	Financial loss; Lack of accountability; Loss of reputation.
Non-Auditability	Poor management; Inability to claim penalties and take legal action.
Loss of Authenticity/Validity	Insufficient patient treatment.

Table 1 - Threats and corresponding impacts; adapted by (Gritzalis, 1998)

The main focus of this chapter is to review and evaluate the privacy challenges introduced by a smart home healthcare environment. For this purpose, both privacy requirements and available solutions are reviewed. In

Section 2, we review privacy requirements for healthcare and, then, we propose a set of requirements for smart home healthcare solutions. In Section 3, we review and discuss existing privacy mechanisms (e.g. architectures, frameworks, models, systems, etc.), like the ones mentioned above. In Section 4, we combine requirements to solutions and produce a mapping of the priorities and goal of each security mechanism found. We conclude our paper by describing key findings, research challenges and future work.

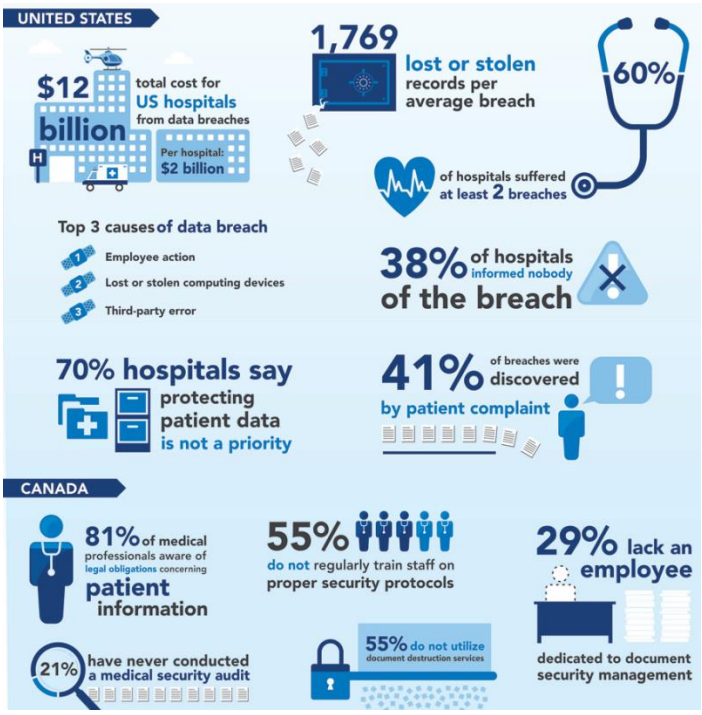

Figure 1 - Privacy in healthcare in numbers[1] (adapted by the Institute for Health Technology Transformation)

2. Privacy requirements for smart home healthcare solutions

2.1 Privacy principles

The US Health Insurance Portability and Accountability Act (HIPAA), passed in 1996 and revised by the American Recovery and Reinvestment Act (ARRA, 2009), identifies privacy rights for patients and required policies for healthcare information systems (HIS) (HHS, 1996). HIPAA includes the following privacy guidelines for privacy compliance and awareness (AMA, 2006; CDT, 2009):

1. Appoint a HIPAA **privacy officer**.
2. Develop "**minimum necessary" policies** for: uses, routine disclosures, non-routine disclosures, limit request to minimum necessary, ability to rely on request for minimum necessary.
3. Develop **policies for access** to designated record set: providing access, denying access.
4. Develop **policies for accounting** of disclosures.
5. Develop **policies for amendment** requests: accepting an amendment, denying an amendment, actions on notice of an amendment, documentation.
6. Develop **policies** for **business associate (BA) relationships** and **amend business associate contracts** or **agreements**: obtain satisfactory assurances in contract, document sanctions for non-compliance.
7. Develop **verification policies**.
8. Develop **policies for alternative means of communication request**.

[1] http://ihealthtran.com/wordpress/2013/06/infographic-protecting-patient-privacy-how-important-is-it/

9. Develop **policies for restricted use request**.
10. Develop **complaint policies**.
11. Develop **anti-retaliation policies**.
12. Develop appropriate **administrative, technical and physical safeguards**.
13. **Train workforce**: train staff, develop sanctions for non-compliance.
14. Develop and disseminate **privacy notice**.
15. **Limit disclosures** to those that are authorized by the client, or that are required or allowed by the privacy regulations.

(Kotz et al., 2009) study several available frameworks (see Table 2): ONC National Framework (HHS, 2008), Health Privacy Project - Best Practices (HPP, 2007), Markle Foundation's "Common Framework" (Markle, 2008), and CCHIT's Certification Criteria (CCHIT, 2008).

No	ONCNF	HPPBP	MFCF	CCHIT	Requirements
1	Individual access	Transparency and notice	Openness and transparency	Consent	Openness and transparency
2	Correction	Education	Purpose specification	Controlling access to your information	Purpose specification
3	Openness and transparency	Employees can choose which content is included in the PHR	Collection limitation and data minimization	Conditions of use	Collection limitation and data minimization
4	Individual choice	Employees control access to and use of the PHR	Use limitation	Amending the record	Use limitation
5	Collection, use, and disclosure limitation	Employees can designate proxies to act on their behalf	Individual participation and control	Account management	Individual participation and control
6	Data quality and integrity	"chain of trust": information policies extend to business partners	Data quality and integrity	Document import	Data quality and integrity
7	Safeguards	Data security	Security safeguards and controls	Data availability	Security safeguards and controls
8	Accountability	Data management	Accountability and oversight	-	Accountability and remedies
9	-	Enforcement and remedies	Remedies	-	Patient Access to Data
10	-	Portability	-	-	Anonymity of Presence

Table 2 - Privacy requirements for healthcare

(Avancha et al., 2012), extend the work of (Kotz et al., 2009) and propose a comprehensive list of ten principles and respective properties (see Table 2):

1. **Openness & transparency**: Inform patients, enable patients to review storage and use of their PHI, enable patients to control, through informed consent.
2. **Purpose specification**: Inform Patients, limit collection and storage of PHI, limit use and disclosure of PHI to those purposes previously specified and consented.
3. **Collection limitation & data minimization:** Enable patients to control, through informed consent, limit collection and storage of PHI, limit use and disclosure of PHI to those purposes previously specified and consented.
4. **Use limitation**: Limit use and disclosure of PHI to those purposes previously specified and consented.

5. **Individual participation & control:** Enable patients to review storage and use of their PHI, enable patients to control, through informed consent.
6. **Data quality & integrity**: Provide access to PHI, ensure quality of PHI.
7. **Security safeguards & controls**: Apply suitable technical and managerial countermeasures.
8. **Accountability & remedies:** Support accountability through robust mechanisms, support mechanisms to remedy effects of security breaches or privacy violations.
9. **Patient Access to Data**: Provide access to PHI and
10. **Anonymity of Presence**: Hide patient identity, sensor presence and data-collection activity from unauthorized observers.

In addition, several authors outline other or similar privacy requirements in the context of healthcare, based on the type of information transmitted and the available solutions used for that purpose (e.g. frameworks, devices, models, etc.). Both (Deng et al., 2011) and (Fang and Zhu, 2010) focus on the preservation of the ***unlinkability*** and ***anonymity*** of the transmitted and stored data and the ***content awareness*** of the patient, while the former also points out the ***policy and consent compliance*** of the whole system used, in parallel with security and privacy requirements regarding home healthcare applications in the cloud. In a more descriptive approach, (Gates and Bishop, 2010) result in the following requirements when combining healthcare deliverance via social networks:

- Information (e.g. name, address, social security number, etc.) should **uniquely be associated** with each specific individual (i.e. data sanitization problem).
- Information **should not be disseminated without the consent** of the patient.
- **Governance** issues (e.g. laws, customs, and other matters) may override the previous control.

Regarding privacy in a UbiComp system, (Dritsas et al., 2006) suggest baseline privacy protection principles, originated from (Langheinrich, 2001). Such principles are outlined as follows:

1. **Notice**: Users should always be aware of the collection of their personal data.
2. **Choice & consent**: Users should have the choice of carrying out, or not, of their personal data.
3. **Proximity**: The collection of data from a user device should only occur when the user is present.
4. **Locality**: Processing and access to data should only be done within the space they were collected.
5. **Anonymity & pseudonymity**: Whenever the user's identity is not required or whenever the user does not consent, anonymity or pseudonymity services should be provided for.
6. **Security**: There should be security mechanisms, which provide adequate protection for collected data.
7. **Access & resource**: Access to user data should only be allowed to authorized persons. There should be regulatory means for the protection of a user against non-compliance.

Similarly, (Rui and Lui, 2010) examine the privacy perceptions of both patients and clinicians/practitioners. They examine how access to the data in an EHR system should be managed and controlled. For example, a patient should be able to restrict access to her EHR if she does not want to reveal such information to family members or healthcare providers and, at the same time, the authenticity of EHR with respect to content authentication and source verifiability should be addressed. On the other hand, clinicians should apply mechanisms to obtain patients' information from multiple EHR repositories accurately, securely, and timely. Furthermore, access to historical medical records should be, in general, granted to a practitioner if both the patient's consent and authorization from the respective Care Delivery Organization (CDO) are granted.

(Giannetsos et al., 2011) distinguish privacy, integrity, and policy issues. They describe **privacy** requirements in the form of questions: *who is asking for the data*? (identity), *how much does the data reveal about me*? (granularity), how *long will the data be retained*? (time). Regarding **integrity**, they point out that the adversary can be both an outsider and an insider. As the personal nature of information significantly increases the interest in launching an attack (i.e. data authentication problem), such sensitive data should be delivered with the assurance that no intermediate users have tampered with them. Regarding **policy**, synergy between policies and technologies entails all of the challenges of interdisciplinary cooperation, the included parties should determine

which issues are best addressed by policy or technology, while policy language can be used in order to express users preferences in a readable format, in case of a complex environment.

In a similar approach (Oladimeji et al., 2011), privacy is achieved when (a) the involved applications confer the ownership and control over disclosure to the principal of that information (Venkatasubramanian and Gupta, 2006), and (b) individual patients have high level of control in deciding who accesses their health information, for what purpose, and under what conditions, while (c) the need for information by health-care personnel, whose identities may not be known in advance, can potentially conflict with privacy, in an emergency response situation. Regarding integrity, data transmission potentially increases integrity vulnerability in this domain (Stajano, 2010) as Ubicomp introduces non-traditional data communication interfaces (e.g. touch-screen icons, voice, infrared signals, direct electrical signals, ad-hoc wireless networks, etc.). Thus, the interchange of the EHR over ad-hoc and pervasive communication channels is susceptible to data harvesting by malicious (passive attacker), while data can be distorted by spurious signals from a malicious (active) attacker.

It is equally important to outline which challenges a patient faces regarding health identity and anonymity. (Mohammed et al., 2009) argues that If a record is so specific that not many patients match it, then releasing the data may lead to linking the anonymous HER to a patient. If a sensitive value occurs together with some Quasi-Identifier attributes frequently, then sensitive information can be inferred from such attributes even though the exact record of the patient cannot be identified. (Ahamed et al., 2007) provide two indicative scenarios regarding privacy violation and information leakage in a healthcare context from which they induce the following challenges: (a) patient authorization is needed to access her EHR, but only on a need-to-know basis, while (b) doctors/healthcare service providers hold the right to restrict access to prediction information, which may be kept secret for the sake of analysis and can only be revealed to the patient, upon request, after the end of treatment.

The above mentioned elements of the privacy issue are generally depicted for healthcare systems, but they can be applied to a healthcare environment, as well. A corresponding list of requirements for healthcare in a smart home would include the following requirements (extends (Avancha et al., 2012)):

R1 - Openness and transparency: *Patients should have knowledge about: PHI collected, purpose of use, identity of persons who can access/use it, PHI location, duration of preservation and how to obtain access and control to it.*

R2 - Purpose specification: *The purpose of PHI collection should be specified at the time of collection, while the subsequent use should be limited to those purposes.*

R3 - Collection limitation and data minimization: *Lawful and fair means should be used for PHI collection; collection should be limited to the PHI necessary to carry out the specified purpose. A patient must authorize such an activity and decide on its approval or rejection, while maintaining knowledge of the included parties.*

R4 - Use Limitation: *Information policies and practices should maintain compliance of the involved activities to the initial specified purposes.*

R5 - Individual participation and control: *Patients should control access to their PHI. They need to know: who is storing what information on them, how that information is being used, to whom it is disclosed.*

R6 - Data quality and integrity: *PHI should be collected in correlation with the intended use purposes and be accurate, complete, and up-to-date. Transmitted data must be protected (e.g. vulnerability protection of the used machines) for integrity preservation.*

R7 - Security safeguards and controls: *Adequate safeguards should be in use for the protection of PHI against existing threats (e.g. modification, disclosure, etc.).*

R8 - Accountability and remedies: *Accountability should be retained among the parties responsible for PHI, while remedies should also exist to address security breaches or privacy violations.*

R9 - Patient access to data: *Patients should obtain access to their PHI in a readable electronic format and be able to modify them, while annotating records submitted by others.*

R10 - Patient's location: *The location of the monitored patient should be private and protected against disclosure, deliberate or not.*

R11 - Anonymity of the patient's data: *PHI should be collected and processed in an anonymous way.*

R12 - Unlinkability of the patient's data: *PHI should preserve unlinkability to the patient. A party should not be able to trace back to the patient based on intercepted data. Such a requirement is opposed to the unique records*

problem, where a patient is easily identified due to the uniqueness of her data (e.g. a record is so specific that not many patients match it).

R13 - Law and policy compliance: *Relevant laws, acts, initiatives, etc. (e.g. HIPAA, ARRA), as well as the defined policies should preserve their compliance among all the available elements of the environment (e.g. roles, information, solutions, frameworks, etc.).*

These requirements can be grouped in four main classes: Anonymity and unlinkability (R11 and R12), Policy and law compliance (R2, R3, R4, R13), Patient's control over the data (R1, R5, R9, R10), and Security countermeasures (R6, R7, R8).

3. Privacy solutions for smart homes

While the literature presents few privacy approaches for smart home solutions, some approaches do exist. For example (Park, 2011) proposes a privacy protection framework regarding RFID services that are today used in smart homes. The goal of the framework is to allow patients to control the personal information transmitted via such a service and the following privacy-related safeguards are outlined:

1. Preservation of **confidentiality**, **integrity** and **entity's authorization** through privacy protection systems,
2. Mobile RFID application and content provides detailed **access control mechanisms** that can manage object information, log data, and personal information by user group,
3. Mobile RFID application and contents provision systems:
    a. Communicate with RPS systems through **secure communication paths**.
    b. Provide **auditing functions** with stronger privacy based on the privacy protection policy that each individual user defined in the RPS system.
    c. **Manages personal privacy information** based on the rules that individual users defined in the Rapid Prototyping System while the system operators are obliged to protect personal privacy information in earnest.
    d. Have a mechanism to **negotiate privacy policies** with mobile RFID terminals to prevent them from gathering personal information.

A classification of the privacy levels is also proposed. The range of the privacy level ranges from no provided privacy protection (level 0) to full privacy protection (level 10). Levels 1 to 9 are separated into **low level** (1-3) where most information is disclosed, **medium level** (4-6), where object information and history are disclosed, and **high level** (7-9), where only part of the object information and object category are disclosed).

Regarding cloud oriented healthcare systems, (Rui and Lui, 2010) propose an EHR security reference model that includes privacy preserving solutions on behalf of the patient. The model consists of three core components, i.e. **secure collection and integration**, **secure storage and access management**, and **secure usage model**. Any transmitted information between two parties should be encrypted via established security protocols (e.g. SSL, TLS, IPSec, etc.), while:

- EHR **authenticity and integrity** must be verified through validating the signature of the EHR owner.
- The **structure and format of composite EHR** should be defined in a way that EHR of different formats from different CDO can be easily and correctly integrated into a composite EHR but also data encryption and access control of individual EHRs can be incorporated without compromises.

The conflict between privacy and the need for immediate access to EHR in emergency situations is still an open issue. (Liang et al., 2011) proposed a **privacy-preserving scheme**, called PEC, which transmits patient's data to nearby helpers in emergency situations via the use of Mobile Healthcare Social Networks. More specifically, it collects all the emergency data (e.g. location, health record, physiological condition, etc.) and establishes a call to the nearby physician by transmitting the gathered information. The security benefits of such approach focus on the guarantee of the availability of the patient's PHI in parallel with the preservation of her privacy. PEC uses encryption to hide transmitted information (generation phase) on the patient's side, while a decryption operation (verification phase) on the PHI by itself is performed on the physician's side.

A similar solution for emergency situations is proposed by (Fang and Zhu, 2010) and is based on **anonymous credentia**l, **pseudorandom number generator (PRNG)**, and **proof of knowledge**. A commitment phase, a signature phase, and a credential derivation phase are used to create anonymous credentials. PRNG reduces the extra communication and storage overhead incurred in encrypting the entire data, while proof of knowledge provides assistance when it is necessary to retrieve data regarding the patient's condition from the PRNG (emergencies).

(Gritzalis, 2004) propose **Privacy Protector (PP)** for HIT systems, which can be used to embed Privacy Enhancing Technologies (PET) in the development process of an application. The approach includes (a) mediation of a privacy protection conceptual entity, which renders the user capable of withholding his real identity, (b) Simplicity of the underlying infrastructure, provided that PP services are embedded within the IT application development process, (c) limitation in the number of trusted entities, since a user has to trust only the is he is currently making use of, (d) limited exposure of personal data to unprotected communication lines, (e) control and responsibility of protecting personal data lies with the user, and (f) an easy-to-apply legal framework.

(Tentori et al., 2006) focus on privacy through the use of ubiquitous computing within a hospital environment, an approach that could be transferred in a ubiquitous smart home, as well. An architecture is proposed which allows the identification of different levels of the **Quality of Privacy (QoP)**, similarly to the Quality of Service (QoS) concept. More specifically, the user demands a certain level of QoP, which is based on contextual variables and the degree of privacy desired while using the ubiquitous application. The architecture is supported by:

- An **ontology** to manage QoP consisting of events, conditions and actions.
- An **agent**, called broker, which handles the communication between the users.
- A context-aware privacy **c-filter**, which filters the communication between the user and the broker.
- A context-aware privacy **s-filter**, which filters the communication between the broker and other agents (e.g. services, devices, etc.).
- A **protocol** to preserve privacy, based on the extension of the SALSA framework (Rodriguez et al., 2005).
- And a **location-aware migration component**, based on (Amaya et al., 2005), which allows users to seamlessly transfer information to any device in the vicinity (e.g. PC).

(Bhatti and Grandison, 2007) propose a privacy management architecture, called PRIMA, which focuses on using policy refinement techniques to improve the coverage of the privacy policy. While this approach is not healthcare specific, it addresses the policy coverage problem in healthcare (i.e. Break the Glass), which is due to the over-reliance on the bypassing of security controls to access sensitive medical information. Further approaches include generic security recommendations for privacy in smart homes. For instance, (Katzenbeisser and Petkovic, 2008) comment on how the use of privacy enhanced protocols protect patient's privacy among e-health services that are either bound to traditional healthcare privacy laws (e.g. HIPAA), or not. Similarly, individual security countermeasures are proposed in (Giannetsos et al., 2011; Fang and Zhu, 2010):

- Anonymity: Anonymization techniques, enhanced user control, decision making, participatory design
- Integrity: Data validation, keyed secure hash function, digital signatures, group signatures, verification protocols, symmetric-key-based message authentication code, watermarking techniques
- Confidentiality: Link/Network layer encryption, access control
- Unlinkability: Produce ciphertexts that appear random

4. Evaluation of privacy in smart home healthcare solutions

In the previous sections we defined privacy requirements for smart home healthcare environments and reviewed existing privacy solutions for this context. Table 3 maps the reviewed solutions/frameworks to privacy requirements. Note that some solutions imply other requirements, but such information was not present or clear and it is not depicted on the table. The table serves as a tool for identifying research priorities and challenges.

Data quality and integrity (R6) and *security safeguards and controls (R7)* are considered as top priority, mainly because they derive by other fields of information security, which do not focus mainly on privacy. Purpose specification (R2), and protecting the patient's location (R10), remain the least addressed requirements. The proposed solutions can be applied to several healthcare technological solutions, including smart homes.

Requirement / Privacy Framework/Solution	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13
National Framework (HHS, 2008)	×			×		×	×	×	×				
Health Privacy Project (HPP, 2007)				×	×		×	×	×				
Common Framework (Markle, 2008)	×	×	×	×	×	×	×	×					
Certification Criteria (CCHIT, 2008)	×			×	×				×				
Mhealth Privacy Framework (Avancha et al., 2012)	×	×	×	×	×	×	×	×	×				
RFID Privacy Protection Framework (Park, 2011)						×	×						×
EHR Security Model (Rui and Lui, 2010)			×	×		×	×						
Privacy-preserving Scheme (Liang et al., 2011)						×	×			×	×		
Privacy and emergency response solution (Fang and Zhu, 2010)						×	×	×			×	×	
Privacy Protector (Gritzalis, 2004)				×	×	×	×	×	×		×	×	×
Quality of Privacy (Tentori et al., 2006)						×	×						
Privacy Management Architecture (Bhatti and Grandison, 2007)				×									
Generic Privacy Recommendations (Katzenbeisser and Petkovic, 2008)						×	×						×
(Giannetsos et al., 2011)						×	×				×		
(Fang and Zhu, 2010)						×	×				×	×	
Coverage (%)	26,70	13,40	20,00	53,30	33,30	80,00	86,70	40,00	33,30	6,70	33,30	20,00	20,00

Table 3 – Framework/Solution and Privacy Requirement Map

5. Conclusions

A smart home healthcare environment faces several privacy threats and risks that need to be addressed due to the sensitive nature of the transmitted patient information. This chapter presented the privacy requirements that need to be met in such an environment. Existing privacy research for healthcare has been reviewed, highlighting the challenges in smart home healthcare (e.g. anonymity, integrity, etc.), as well as existing solutions.

Indicative types of smart healthcare technologies include (Athavale, 2011) ***simple devices*** (blood glucometers, blood pressure monitors, oximeters, etc.) which provide standardized outputs for specific physiological conditions, ***intelligent applications or software*** capable of analyzing and processing body signals, ***sensor integrated smart devices*** (smartphones and gaming devices), ***wearable sensors*** (e.g. T-Shirts, wrist straps, etc.) and **other devices** exclusively manufactured for the purpose of body signal monitoring/processing (e.g. mainframe computers, tablets, etc.). Each of these categories poses different challenges when their designers attempt to comply with the above privacy requirements. A comprehensive study of the controls needed in order to achieve each requirement for such device types is the direction that smart home developers need to follow in order to ensure privacy for their solutions. One of the main challenges that need to be addressed is the conflict between legal restrictions, individual human rights and the need for immediate access to a patient's data when his health is at stake, which in the case of smart home entails the violation of the sanctuary of his home. Ultimately, smart (home) healthcare requires a best practice guide, outlining both the technical and procedural countermeasures required in order to maintain privacy, taking into account modern technology environments, such as the cloud, smartphones and ubiquitous equipment, which are gradually incorporated in smart healthcare solutions.

References

Ahamed S I, Talukder N, Kameas A D (2007) Towards Privacy Protection in Pervasive Healthcare. Paper presented at the 3rd International Conference on Intelligent Environments, Ulm, Germany, September 2007

Amaya I, Favela J, Rodriguez M (2005) Componentes de software para el desarrollo de ambientes de cómputo ubicuo. Paper presented at the In the International Ubiquitous Computing and Ambient Intelligence Conference, Granada, Spain, September 2005.

AMA (2006) Checklist for HIPAA Privacy. In: HIPAA Insider. Alabama Medicaid Agency. Available via MEDICAID. http://www.medicaid.state.al.us/old_site/hipaa/Checklist%20for%20HIPAA%20Privacy.pdf. Accessed 9 Sep 2013

ARRA (2009) American Recovery and Reinvestment Act. In: US Government Printing Office. Available via GPO. http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf. Accessed 9 Sep 2013

Athavale Y (2011) Potential applications of smart healthcare technologies. In: SAR-NexJ NSERC Engage Collaboration. Available via SAR-NexJ. http://sarnexj.wikispaces.com/file/view/Potential+applications+of+smart+healthcare+technologies.pdf. Accessed 22 Sep 2013

Avancha S, Baxi A, Kotz D (2012) Privacy in mobile technology for personal healthcare. ACM Computing Surveys 45:1–54

Bhatti R, Grandison T (2007) Towards improved privacy policy coverage in healthcare using policy refinement. Paper presented at the 4th VLDB conference on Secure data management, Vienna, Austria, Springer, September 2007

CCHIT (2008) Consumer's guide to certification of personal health records. In: Certification Commission for Healthcare Information Technology. Available via CCHIT. http://cchit.org/files/CCHITPHRConsumerGuide08.pdf. Accessed 9 Sep 2013

CDT (2009) Summary of Health Privacy Provisions in the 2009 Economic Stimulus Legislation. In: Centre for Democracy and Technology. Available via CDT. https://www.cdt.org/healthprivacy/20090324_ARRAPrivacy.pdf. Accessed 9 Sep 2013

Deng M, Petkovic M, Nalin M, Baroni I (2011) A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges. Paper presented at the 4th International Conference on Cloud Computing, IEEE, USA, July 2011

Dritsas, S., Gritzalis, D,. Lambrinoudakis, C. (2006) Protecting privacy and anonymity in pervasive computing trends and perspectives. Telematics and Informatics Journal, Special Issue on Privacy and Anonymity in the Global Village 23(3):196-210

HPP (2007) Best Practices for Employers Offering Personal Health Records (PHRs). In: Health Privacy Project. Employers' Working Group on Personal Health Records. Available via CDT. https://www.cdt.org/files/pdfs/2007Best_Practices.pdf. Accessed 9 Sep 2013

Fang S J Y, Zhu X (2010) Privacy and emergency response in e-healthcare leveraging wireless body sensor networks. Wireless Communications, IEEE 17.1:66–73

Gates C, Bishop M (2010) The security and privacy implications of using social networks to deliver healthcare. Paper presented at the 3rd International Conference on Pervasive Technologies Related to Assistive Environments, Univ. of Texas at Arlington, USA

Giannetsos T, Dimitriou T, Prasad N R (2011) People-centric sensing in assistive healthcare: Privacy challenges and directions. Security and Communication Networks 4.11:1295–1307

Gritzalis, D. (2004) Embedding privacy in IT applications development. Information Management and Computer Security Journal 12(1):8-26

Gritzalis, D., Lambrinoudakis, C. (2004) A Security Architecture for Interconnecting Health Information Systems. International Journal of Medical Informatics 73:305-309

Gritzalis, D. (1998) Enhancing security and improving interoperability in healthcare information systems. Medical Informatics 23(4):309-324

Gritzalis, D. (1997) A baseline security policy for distributed healthcare information systems. Computers & Security 16(8):709-719

Health & Human Services U.S. Department (2008) Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information. In: Privacy & Security Policy. Health & Human Services U.S. Department.

Health & Human Services U.S. Department (1996) The Health Insurance Portability and Accountability Act. http://www.hhs.gov/ocr/privacy/index.html. Accessed 9 Sep 2013

Katzenbeisser S, Petkovic M (2008) Privacy-preserving recommendation systems for consumer healthcare services. Paper presented at the 3rd International Conference on Reliability and Security, Technical University of Catalonia, Spain, March 2008

Kotz D, Sasikanth A, Amit B (2009) A privacy framework for mobile health and home-care systems. Paper presented at the 1st ACM workshop on Security and privacy in medical and home-care systems, Chicago, IL, USA, ACM, November 2009

Langheinrich M (2002) A Privacy Awareness System for Ubiquitous Computing Environments. Ubiquitous Computing 206:237–245

Langheinrich M (2001) Privacy by design - principles of privacy - aware ubiquitous systems. In the 3rd International Conference on Ubiquitous Computing, September 2001. Lecture Notes in Computer Science, vol. 2201. . Springer, Heidelberg, pp. 273–29.

Lekkas, D., Gritzalis, D. (2006) Long-term verifiability of healthcare records authenticity. International Journal of Medical Informatics 76(5-6):442-448

Liang X, Lu R, Chen L, Lin X, Shen X (2011) PEC: A privacy-preserving emergency call scheme for mobile healthcare social networks. Journal of Communications and Networks 13.2:102–112

Markle (2008) Common Framework for networked personal health information: Overview and principles. In: Connecting for Health. Markle Common Framework. Available via MARKLE. http://www.markle.org/sites/default/files/CF-Consumers-Full.pdf. Accessed 9 Sep 2013

Mohammed N, Fung B C M, Hung P C K, Lee C (2009) Anonymizing healthcare data: a case study on the blood transfusion service. Paper presented at the 15th ACM International Conference on Knowledge Discovery and Data mining, France, ACM, June 2009

Oladimeji E A, Chung L, Jung H T, Kim J (2011) Managing security and privacy in ubiquitous eHealth information interchange. Paper presented at the 5th International Conference on Ubiquitous Information Management and Communication, ACM, Korea, February 2011

Park N (2011) Customized Healthcare Infrastructure Using Privacy Weight Level Based on Smart Device. Convergence and Hybrid Information Technology 206:467–474

Rodriguez M, Favela J, Preciado A, Vizcaino A (2005) Agent-based Ambient Intelligence for Healthcare. AI Communications 18(3):10–16

Rui Z, Liu L (2010) Security models and requirements for healthcare application clouds. Paper presented at the 33rd International Conference on Cloud Computing, USA, July 2010

Stajano F (2010) Security Issues in Ubiquitous Computing. In: Nakashima H, Aghajan H, Augusto J C (ed). Handbook of Ambient Intelligence and Smart Environments, vol 3. Springer, pp 281-314

Tentori M, Favela J, González V M (2006) Quality of Privacy (QoP) for the Design of Ubiquitous Healthcare Applications. Journal of Universal Computer Science 12.3:252–269

Venkatasubramanian K, Gupta S K S (2006) Security Solutions for Pervasive Healthcare. Paper presented at the 3rd International Conference on Security in Pervasive Computing, UK, April 2006