Privacy issues in smart home healthcare environments

Nikolaos Tsalis

ntsalis@aueb.gr

Information Security & Critical Infrastructure Protection Research Laboratory

Dept. of Informatics, Athens University of Economics & Business (AUEB), Greece

Health Insurance Portability And Accountability Act (HIPAA) policies

- ❑ Appoint privacy officer
- ❑ Minimum necessary
- ❑ Access to designated record set
- ❑ Accounting disclosures
- ❑ Amendment requests
- ❑ Business associates
- ❑ Verification
- ❑ Alternative means of communication request
- ❑ Restricted use request
- ❑ Complaint
- ❑ Anti-retaliation
- ❑ Safeguards
- ❑ Train workforce
- ❑ Privacy notice
- ❑ Limit disclosures

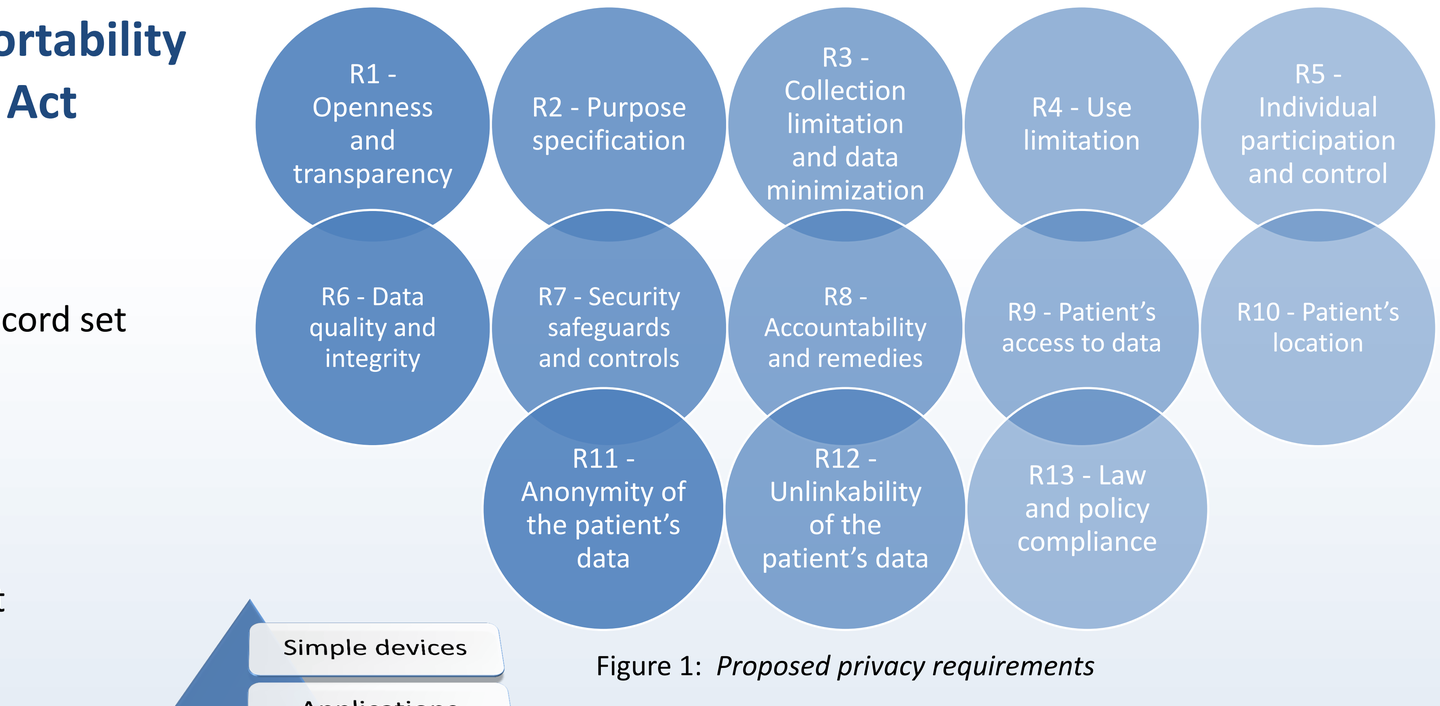


Figure 1: *Proposed privacy requirements*

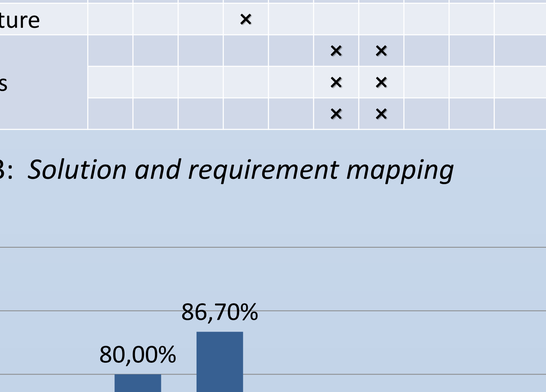


Figure 2: *Indicative smart home solutions*

Methodology

- ❑ Identification of existing requirements regarding healthcare environments
- ❑ Review of available privacy preserving solutions
- ❑ Proposal of privacy requirements (c.f. Figure 1)
- ❑ Mapping of solutions and requirements (c.f. Figure 3)
- ❑ Identified requirement coverage (c.f. Figure 4)

Privacy Solution / Requirement	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13
National Framework	×			×		×	×	×	×				
Health Privacy Project				×	×		×	×	×				
Common Framework	×	×	×	×	×	×	×	×					
Certification Criteria	×			×	×				×				
Mhealth Privacy Framework	×	×	×	×	×	×	×	×	×				
RFID Privacy Protection Framework						×	×						×
EHR Security Model			×	×		×	×						
Privacy-preserving Scheme						×	×			×	×		
Privacy and emergency response solution						×	×	×			×	×	
Privacy Protector				×	×	×	×	×	×		×	×	×
Quality of Privacy						×	×						
Privacy Management Architecture				×									
Individual security solutions						×	×						×
						×	×				×		
						×	×				×	×	

Figure 3: *Solution and requirement mapping*

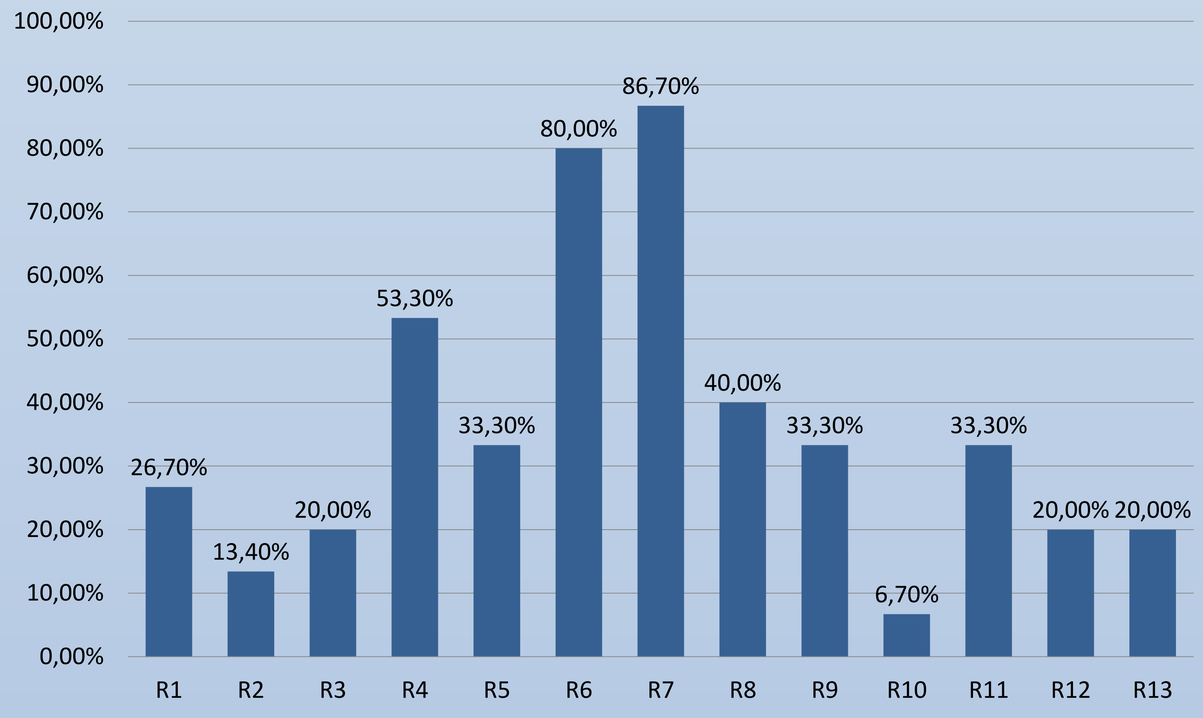
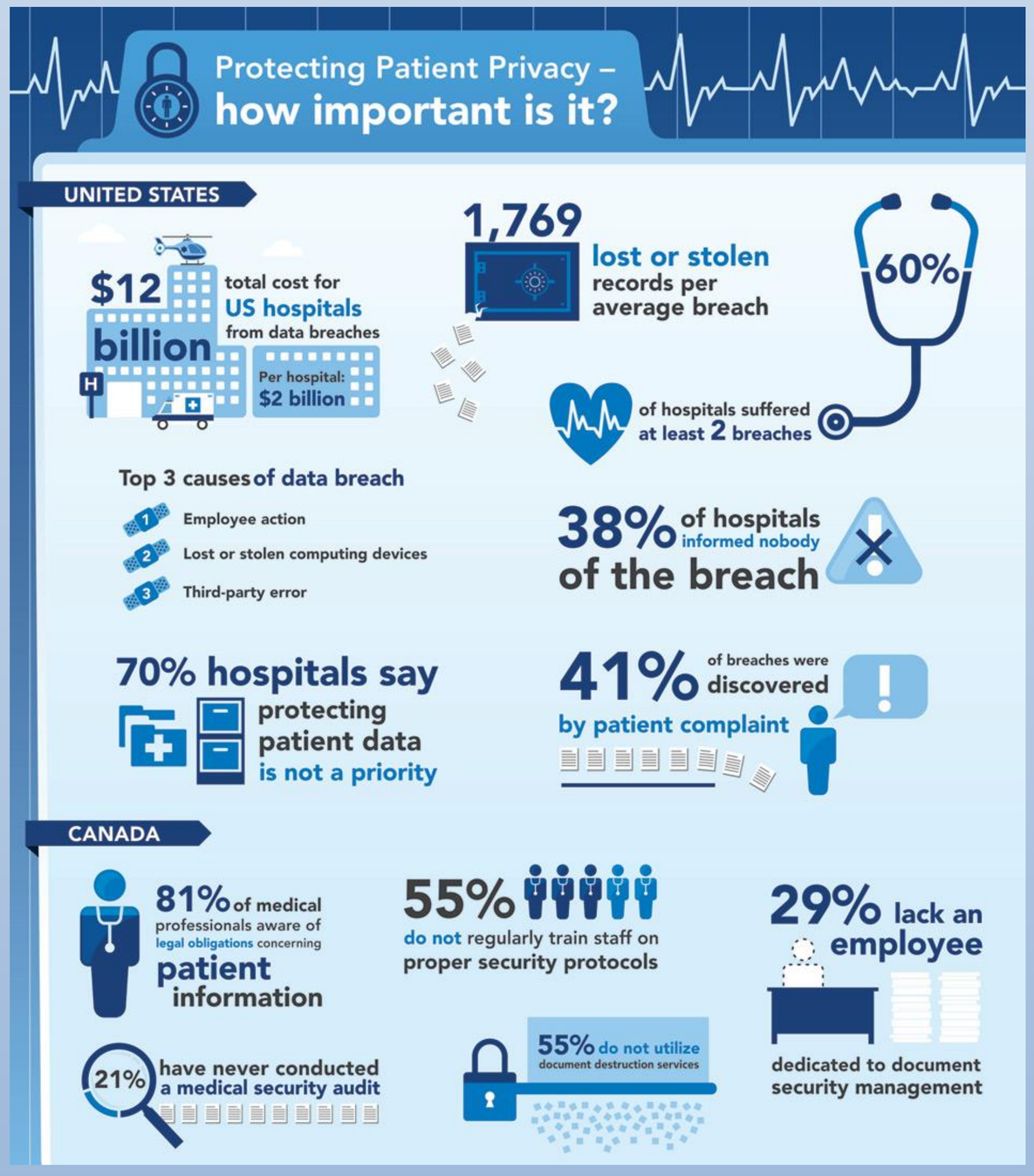


Figure 4: *Requirement coverage*

No	ONC	BP	CF	CCHIT	MH
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

Figure 5: *Privacy frameworks' requirements for healthcare*



References

1. 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.
2. Avancha S, Baxi A, Kotz D (2012) Privacy in mobile technology for personal healthcare. ACM Computing Surveys 45:1–54.
3. Gritzalis D., "A baseline security policy for distributed healthcare information systems", Computers & Security, Vol. 16, No. 8, pp. 709-719, 1997.
4. Gritzalis D., "Embedding privacy in IT applications development", Information Management and Computer Security, Vol. 12, no. 1, pp. 8-26, MCB University Press, 2004.
5. Gritzalis D., "Enhancing security and improving interoperability in healthcare information systems", Informatics for Health and Social Care, Vol. 23, No. 4, pp. 309-324, 1998.
6. Gritzalis D., Lambrinoudakis C., "A Security Architecture for Interconnecting Health Information Systems", International Journal of Medical Informatics, Vol. 73, pp. 305-9, 2004.
7. 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.
8. Kandias M., Virvilis N., Gritzalis D., "The Insider Threat in Cloud Computing", Proc. of the 6th International Conference on Critical Infrastructure Security, pp. 93-103, Springer (LNCS 6983), 2013.
9. Kotz D, Sasikanth A, Amit B (2009) A privacy framework for mobile health and home-care systems. Proc. of the 1st ACM Workshop on Security and privacy in medical and home-care systems, ACM, USA, 2009.
10. Lekkas D., Gritzalis D., "Long-term verifiability of the electronic healthcare records' authenticity", International Journal of Medical Informatics, Vol. 76, Issue 5-6, pp. 442-448, 2006.
11. Lekkas D., Gritzalis D., Cumulative notarization for long-term preservation of digital signatures, Computers & Security, Vol. 23, no. 5, pp. 413-424, 2004.
12. Soupionis Y., Gritzalis D., "Audio CAPTCHA: Existing solutions assessment and a new implementation for VoIP telephony", Computers & Security, Vol. 29, No. 5, pp. 603-618, 2010.