CERIAS

the center for education and research in information assurance and security

Human Factors Considerations for Privacy Properties in Home Healthcare Systems

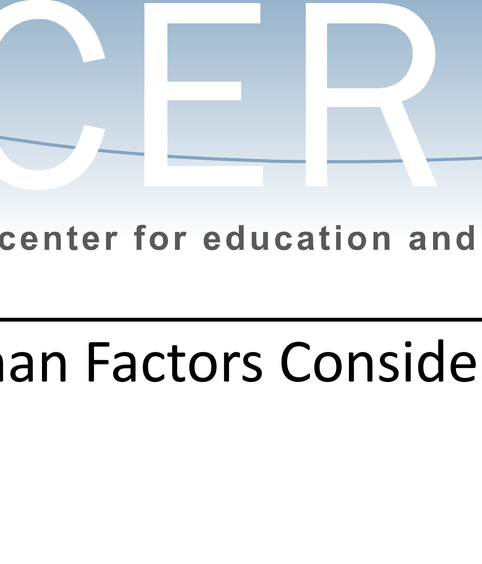
Kyeong-Ah Jeong & Robert W Proctor

Dept. of Psychological Sciences

Purdue University

Abstract

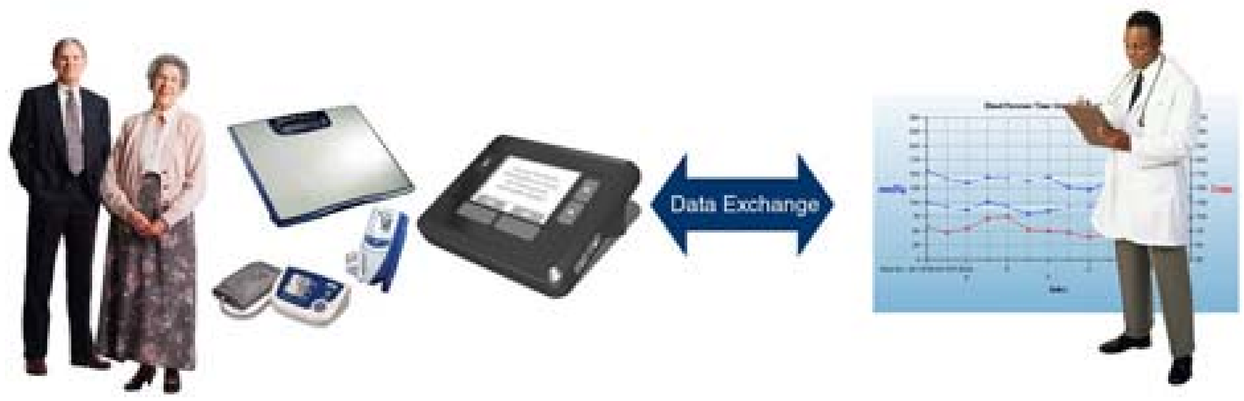
Privacy properties for remote/home-based healthcare systems have been proposed, but human factors issues involved in implementing those properties have received little consideration. We reviewed proposed privacy properties and identified human factors issues associated with successful implementation of these properties. Implementations that do not take the users into account will most likely fail to accomplish their privacy and security goals.



Privacy Properties for Home Healthcare

(Kotz, Avancha, & Baxi, 2009)

1. Inform patients about all aspects of privacy and security concerning their personal health information (PHI).
2. Enable patients to review how their PHI is stored and used.
3. Enable patients to control what data will be collected and when, who will have access, and how it can be used.
4. Enable patients to access their PHI so that they can request changes and corrections to entries.
5. Provide easy-to-use interfaces that allow patients to be able to find out as much detailed information as they desire.
6. Limit collection and storage of PHI to conform to the patient's consent and as needed for specified purposes.
7. Limit use and disclosure of PHI to those purposes previously consented to.
8. Ensure accuracy, integrity, and authenticity of PHI.
9. Conceal patient identity, the presence of sensors, and data collection activity from unauthorized observers.
10. Support accountability through robust audit log mechanisms that track every transaction.
11. Support mechanisms to remedy effects of privacy violations.



Human Factors Recommendations for Privacy Properties in Home Healthcare Systems

General: Without being designed for use by all stakeholders (e.g., patient, provider), the privacy provided by remote/home healthcare systems will be less than desired.

Privacy Property 1: The privacy policy and consent materials must be aimed toward the user's abilities and concerns, allowing effective communication.

Privacy Properties 2, 3, and 4: The username-password combination is an acceptable authentication method for many purposes, because it is easy to implement and has high user familiarity and acceptance.

- Various ways to improve the security provided by passwords, while making them memorable for users, should be implemented.
- Special characteristics of patients must be considered.
- Stronger forms of authentication, though possibly less usable, should be used for situations in which the users are trained personnel and security is very critical.

Privacy Property 5: Users' perception and performance with the interface should be evaluated with respect to different design variables (e.g., type of users, situations of use, the PHI involved, and the technologies used).

- Older and/or disabled patients' cognitive and physical capabilities should be addressed to ensure the patients' autonomy.

Privacy Properties 6, 7, and 10: Issues regarding intrusion detection need to be addressed. Regular inspection of system audit logs is necessary, but better methods need to be developed that allow system administrators to easily detect changes in data and unusual usage patterns.

Privacy Property 8: Various ways of reducing human errors and mistakes in data entry and modification should be considered and implemented.

- For control of the information, patients' misunderstandings may result in their failing to give consent to inclusion of critical PHI in their record

Privacy Property 9: Sensors should be designed for usability by patients.

- Issues include how best to alert patients when recording systems are activated.

Reference

Kotz,, D., Avancha, S., & Baxi, A. (2009). A privacy framework for mobile health and home-care systems. In *Proceedings of the First ACM Workshop on Security and Privacy in Medical and Home-care Systems* (pp. 1-12). New York: ACM.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center