User Centred Networked Health Care
A. Moen et al. (Eds.)
IOS Press, 2011

doi:10.3233/978-1-60750-806-9-606

Personal Health Information on Display: Balancing Needs, Usability and Legislative Requirements

Erlend Andreas GJÆRE [a], Inger Anne TØNDEL [b, 1], Maria B. LINE [b],
Herbjørn ANDRESEN [c], Pieter TOUSSAINT [a]
[a] *Dep. of Computer and Information Science, NTNU, Trondheim, Norway*
[b] *SINTEF ICT, Trondheim, Norway*
[c] *Dep. of Private Law, University of Oslo, Norway*

Abstract. Large wall-mounted screens placed at locations where health personnel pass by will assist in self-coordination and improve utilisation of both resources and staff at hospitals. The sensitivity level of the information visible on these screens must be adapted to a close-to-public setting, as passers-by may not have the right or need to know anything about patients being treated. We have conducted six informal interviews with health personnel in order to map what kind of information they use when identifying their patients and their next tasks. We have compared their practice and needs to legislative requirements and conclude that it is difficult, if not impossible, to fulfil all requirements from all parties.

Keywords. Personal health information, de-identification, privacy, coordination

1. Introduction

The COSTT[2] project aims at supporting coordination in the peri-operative hospital environment by visualising status information regarding current operations and patients under treatment on large wall-mounted screens. This will help the personnel predicting when their time and effort are needed, and which colleagues are available for advice or assistance. As a result, both physical resources and staff can be utilised more effectively. Research on similar computerised coordination systems implemented as electronic whiteboards are also presented by Bardram et al. [1] and Aronsky et al. [2]. In order to maximise coordination support, the screens should be placed at locations where the relevant health personnel are likely to see them, e.g. in corridors. This however makes them available to everybody present, including patients, their relatives, and personnel not directly involved in patient treatment (e.g. cleaners and technicians). Such availability has consequences for the privacy of patients and employees.

In previous work [3] we have introduced the concept of *flexible de-identification*, and described how it is possible to present patient information at various levels of

[1] Corresponding author: Inger Anne Tøndel, SINTEF ICT, N-7465 Trondheim, Norway; E-mail: inger.a.tondel@sintef.no

[2] Co-operation support Through Transparency, http://costt.no/

details, both with regards to identifying information and the medical condition. Three perspectives have to be taken into account when developing solutions for de-identification. The first perspective is that clinical personnel require a certain amount of identifying information for the medical information presented to be meaningful and useful. The second perspective is that laws and regulations restrict the amount of patient identifying information that can be presented. The last perspective is usability. A system that requires users to log on to multiple systems in order to obtain patient information, might fulfil both the information need and requirements set by laws and regulations, but is not very usable in a dynamic work environment where clinicians work under time pressure. These three perspectives generate different demands, and designing the right level of de-identification means balancing these different demands.

The rest of the paper is organised as follows: Section 2 presents the results of unstructured interviews with personnel working in the surgical clinic at a Norwegian hospital, and Section 3 outlines the Norwegian legislative requirements. Then, Section 4 discusses how needs, usability and legislative requirements can be balanced, and Section 5 concludes the paper.

2. Interviews

In order to improve our understanding of the information needs of health care personnel, and specifically their need for identifying information, we conducted six unstructured interviews at Trondheim University Hospital, during November-December 2010. Six different identification approaches were explored (see overview in Table 1), where the one with highest identification level used initials and birth year of the patient. The less identified approaches aimed to identify the patient by his location or his relation to health care personnel, possibly in combination with the test or surgery type performed. In the interviews we wanted to gain feedback on whether the less identifying approaches still resulted in useful status information for health care workers.

The participating clinicians included one senior physician and two ward nurses from the Department of Gastrointestinal Surgery, one junior physician and one nurse from the Department of Emergency, one ward nurse from the Department of Breast and Endocrine Surgery, and one charge nurse from a ward at the Department of Orthopaedic Surgery. Their ages ranged from 25 to 55, and all had been in their position for some while. The informants were recruited randomly during work hours, and interviewed straight away in their regular work environment. They were each asked to comment on some early-stage paper-based prototypes of information visualizations, containing message examples related to the treatment progress of patients, e.g. “CT-image description is ready” and “Patient has been scheduled for surgery”. We explored in total four different prototypes, but only one or two were presented to each informant. Some status messages were added during the process, and two of the prototypes were modified slightly in-between interviews, due to feedback given. The prototypes mainly differentiated on how information was organised and how the patients were identified). We used the prototypes to investigate whether the clinicians would be able to tell patients’ identities apart with the different identification approaches, and to evaluate how these related to current practices. The feedback was recorded with handwritten field notes, and written out directly afterwards.

The results of the interviews are summarised in Table 1. Generally, clinicians were positive to the idea of integrating status updates from several systems. Most were still reluctant to the immediate thought of placing *any* patient information more publicly available than workstations or personal devices. Though the approach where patients are identified by initials and birth year stood out as the most convenient option, our main impression is that health care personnel have varying needs for patient identification, depending on their role and the context where identification should happen. We also discovered that clinicians commonly used patients' diagnosis or treatment history as de-identification in conversations between colleagues, (e.g. "he with ileus who needs another operation in three days").

Table 1. De-identification approaches explored in the interviews, based on the paper-based prototypes.

Approach	Example	Summary of Responses
Initials and birth year of patient	JD59	Will normally provide fairly good accuracy. Patients having the same birth year and initials (or last name) do however occur. Clinicians still found this convenient as they are used to working with basis in the patients and their name/age (various combinations of name and birth date are used today).
Room number/location	*(Plotted on a map of wards)*	Patients move around (this may leave room lists temporarily inconsistent) or they can even be placed in the corridors. Room numbers are commonly used for reference today, but in combination with other identifiers, e.g. name, diagnosis or sex. It seems hard to remember the patients' exact locations.
Initials of responsible physician *(first two letters of both first name and last name)*	DAJO	Patients are not followed up by only one physician, and physicians attend many patients at each ward. Nurses will not necessarily know the name of the physician providing care for each of their patients at a specific time.
Blood test indicators, time and responsible nurse	Hb, Na, INR 10:41 (HAPE)	Blood tests are ordered as standardised batches, so important indicators, if any (e.g. INR may decide whether to operate or not), do not stand out. Tests for several patients are often ordered at the same time, and by the same nurse, too.
Radiology type, level of urgency, time and referring physician	CT abdomen (red) 11:00 (DAJO)	Some results (MR) take days to arrive, and often 20-30 patients with abdominal pains arrive daily. Hence, a list of pending results may become overloaded and hard to interpret.
Operation room number, surgery type, scheduled time and surgeon initials	OP3: Appendicitis 11:00 (PT)	Nurses rarely know exactly what room an operation will take place in. But as it is uncommon to have several patients from the same ward undergoing surgery at the same time, they may still be able to deduce which operation to follow.

3. Legislative Requirements

In Norway, rules and regulations on the obligation of secrecy, and the criteria for sharing or disclosing data, are mainly found in the Personal Health Data Filing System Act [5] which implements the EU personal data protection directive [4] for the health domain, and in the Health Personnel Act [6] which are national rules of conduct for health personnel. The authorisation rule for granting access to health data [5] consists mainly of two criteria. The first is a general need-to-know restriction: "Access may only be granted insofar as this is necessary for the work of the person concerned" [5]. The second criterion is that access must be "in accordance with the rules that apply regarding the duty of secrecy" [5]. The general rule on secrecy goes beyond a mere duty to "keep silent". It is a proactive duty on institutions as well as individual health personnel to "prevent others from gaining access to or knowledge of information relating to people's health or medical condition" [6]. There are a few derogations to the secrecy rule [6], mainly the need to share information with co-operating health personnel, the duty to supply patient administrative systems with key data, and a few more rules on sharing information with a patient's next of kin, and with students, health care assistants or data processing expertise. However, there are no general permissions for making health data available to *other* patients, or to other patients' next of kin.

There are, in principle, two possible strategies on how to make the envisioned wall-mounted displays legitimate under data protection law. The first strategy would be to generalise or trivialise the data in ways that put the information content below the threshold of "relating to people's health or medical condition". An example could be to make the displayed data read something like "patient x to be present in room 101 from 9:30 to 14:00" without revealing what activities would take place there. The second strategy would be some sort of de-identification of the patient, in order to avoid that the displayed data pertains to a specific part of the definition of "personal health data" [5], namely a criterion that it "may be linked to a natural person".

Norwegian law contains several useful concepts for de-identification [5]. These legal concepts were initially aimed at central health registers, spanning information originating from different hospitals, but they could also be relevant for de-identification purposes within a single hospital. The definition of "de-identified personal health data" has two components. First, any identifying data is removed. Second, any re-identification shall be *dependent* on re-supplying the data that was removed. This second component implies a high threshold; an acceptable level of de-identification may not be pro forma, and re-linking data to the right patient cannot be easily accomplished by guessing. An alternative is to aim for "pseudonymous health data", which implies that identifying information is encrypted.

4. Discussion

The interviews indicate that status updates for patients under treatment are useful. Health care personnel would like to know when test results are ready, how operations proceed, etc. Making such information easily available on wall-mounted screens will however expose the information to everybody who has physical access, something that is not permitted by Norwegian legislation. As mentioned in Section 3, two main strategies are available in order to adhere to the legal restrictions: Removing all health-related information or de-identifying the information. The first strategy may work for some events, but using it as a general strategy, will probably render the system useless. The second strategy seems more appealing, as it can supply more useful information. Finding an appropriate level of de-identification that makes personnel able to identify patients yet remains a challenge.

Results from the interviews reveal that variations over name and birth date are commonly used for identification. At a ward with a limited number of patients, this close to identifies most patients. The other de-identification techniques tested in the interviews, such as using the room number or the identity of health care personnel, turned out not to be usable. Thus we need to work on alternative de-identification methods. Existing literature on de-identification of health information [7] is mainly concerned with de-identification of large datasets that are to be used for secondary purposes (e.g. research). Still we plan to look into how existing techniques such as pseudonymisation can be used for our setting. We will also investigate to what extent information will still be useful if all identifiers are removed.

If it turns out that the level of de-identification required by legislation will render the system useless, we are left with no option but to limit access to the information to authorised personnel only. This can be ensured by placing the screens at locations where only health personnel have access or by access control mechanisms on the screens, although this will exceedingly reduce the usability for coordination purposes. If such an approach is necessary, it will be important to investigate smart ways of doing access control, e.g. by providing more details on a personal handheld device, or by mechanisms that automatically detect who is present and present information based on the access rights of that group of people.

Reducing the level of identification will result in an increased risk of erroneous interpretation of information. Though this will reduce the benefits of the coordination support system, it is important to state that the system will not replace any of the medical information systems. These will still use full identification for all medical data, and thus there should be no increased risk of treatment errors.

5. Conclusion

Public display of health information poses an obvious risk to patient privacy, and thus there is a need to determine the appropriate level of identification. As the legislative requirements are in conflict with the needs of health personnel, it may be impossible to fulfil all the legislative requirements, without sacrificing usability.

Acknowledgments: We would like to thank Børge Lillebo for his work on the prototypes and cooperation on the interviews. Thanks also to our other colleagues in the COSTT project, Arild Faxvaag especially, for useful comments and discussions. This work was supported by the Norwegian Research Council's VERDIKT program (grant no. 187854/S10).

References

[1] Bardram, J.E. Hansen, T. Soegaard, M. AwareMedia – A Shared Interactive Display Supporting Social, Temporal, and Spatial Awareness in Surgery, *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work (CSCW '06)* (2006), 109-118.

[2] Aronsky, D. Jones, I. Lanaghan, K. Slovis, C.M. Supporting Patient Care in the Emergency Department with a Computerized Whiteboard System, *Journal of the American Medical Informatics Association* **15** (2008) , 184-193.

[3] Faxvaag, A. Røstad, L. Tøndel, I.A. Seim, A.R. Toussaint, P.J. Visualizing Patient Trajectories on Wall-Mounted Boards – Information Security Challenges, *Studies in Health Technology* **150** (2009), 750-759.

[4] 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

[5] Act on personal health data filing systems and the processing of personal health data [Personal Health Data Filing System Act]

[6] Act of 2nd July 1999, no 64 relating to health personnel etc. [The Health Personnel Act]

[7] El Emam, K. Fineberg, A. An overview of Techniques for De-identifying Personal Health Information, Health Canada, January 2009.