Visualizing Patient Trajectories on Wall-Mounted Boards – Information Security Challenges

Arild FAXVAAG [a,1], Lillian RØSTAD [b], Inger A. TØNDEL [b], Andreas R. SEIM [c], Pieter J. TOUSSAINT [c]

[a] *The Norwegian EHR Research Centre (NSEP), Institute of Neuroscience, Faculty of Medicine, Norwegian university of science and technology, Trondheim, Norway*

[b] *SINTEF ICT, Trondheim, Norway*

[c] *Department of Computer and Information Science, Faculty of Information Technology, Mathematics and Electrical Engineering, NTNU, Trondheim, Norway*

Abstract. Since operating room departments are among the costliest resources at a hospital, much attention is devoted to maximize their utilization. Operating room activities are however notoriously hard to plan in advance. This has to do with the unpredictable, problem-solving nature of the work and that the work is carried out by a multidisciplinary team of health personnel, members of which also have commitments outside the operating room department. We assume that operating room teams have the capacity to coordinate themselves and that coordination might be facilitated by visualizing relevant information on wall-mounted boards. To characterize clinical situations that require coordination and re-planning of the teams' work, we have developed a realistic scenario. We analyse and discuss the information security challenges that follow from displaying information on the whereabouts of other teams, actors and patients on wall-mounted boards in the operating rooms. Information security threats could be mitigated by de-identification techniques. Information demands could thereby be met without sacrificing the privacy of those whose information is displayed.

Keywords. coordination in healthcare, workflow support, clinical process, patient trajectory, healthcare planning

1. Introduction

Collaboration in health care is best characterized as team problem solving. Planning such an activity, monitoring its progress and supporting the collaboration by means of ICT, is a difficult task due to the rather unpredictable course that these activities take. However, proper collaboration is essential because it can prevent expensive process breakdowns that may jeopardize patient safety. In order to support collaboration in health care in a way that is properly aligned to the character of clinical work, we started a large research project called COSTT (Co-Operation Support Through Transparency). It is a four-year project funded by the Norwegian research council, has an overall budget of approximately 3.3 million Euros, and started in September 2008.

[1] Corresponding Author: Arild FAXVAAG, The Norwegian EHR Research Centre, Medical-Technical Research Centre, N-7489 Trondheim, Norway; E-mail: arild.faxvaag@ntnu.no.

Our basic assumption is that traditional workflow oriented approaches are ill suited for supporting collaboration in clinical processes [1]. Instead, we believe the solution lies not in controlling the flow of work, but in providing all actors involved with visualizations that provide an easily accessible and comprehensive overview of the progress of a process and its current status. By making the process transparent to all those involved, the actors can better coordinate their work. Coordination is facilitated but not forced upon the health care workers.

The core concept in our visualization of the progress and current status of a clinical process is the *patient trajectory* – a timeline-oriented representation of what actually has happened with the patient during encounters with clinicians [2]. By inspecting a patient trajectory, a clinician can see how far the plan concerning a patient has progressed, and also whether there have been deviations from the plan. Based on this information he can decide if he needs to make any changes in his own planned activities.

We aim to construct such visualization on the basis of data that are collected automatically in the perioperative domain from "sensors" in both digital and physical reality. Examples of digital sources are the information systems that are in use, such as Electronic Patient Records and scheduling systems. Examples of physical sources are tracking devices, monitoring devices on the patient, equipment, and the environment.

However, transparent trajectories and visualization of work will present new threats to the privacy of patients and employees. Finding effective ways of mitigating such threats is an important research challenge. In this paper we address two questions pertaining to this research challenge:

1. How can sensitive data be removed from the visualization of a patient's trajectory while still conveying meaning to those with access to the visualization?
2. How must access control policies be extended in order to include access of visualized information by groups?

2. A Scenario

Surgical operations are carried out in operating rooms by multidisciplinary teams that typically include an anaesthesiologist, a nurse anaesthetist, one or two surgeons and two operating room nurses. The exact team composition depends on the surgical procedure that takes place, but may also differ somewhat between countries. The principal role of the operating room nurses is to assist the surgeon(s). The anaesthesia team protects the patient from experiencing pain during the operation and monitors the functions of vital organs.

Since operating rooms are very expensive staff-intensive resources and operating room suits often constitute bottlenecks that limit throughput, much effort is put into optimizing the flow of patients and personnel in perioperative environments. Management of perioperative resources, personnel, and patient flow is typically the responsibility of one or more coordinators in the operating room suite.

Operating room activities are notoriously hard to plan accurately in advance. Diseases present themselves differently from patient to patient. Although the surgeon may have a clear picture of what to expect and how to proceed at the beginning of an operation, he also must understand and react upon unanticipated events. The surgeon might for instance suddenly uncover a lesion that is not related to the disease that is

operated upon. This discovery could force him to postpone the planned surgery until the nature of the lesion has been characterized, something that requires the involvement of the pathology department. The team might alert this department that they will receive a tissue sample from the lesion that must be analyzed immediately. At the same time, the surgeon(s) would take a biopsy and send it to pathology. The operation would then be effectively paused, and would be aborted unless pathology's analysis shows that the lesion is not indicative of cancer. If the operation can continue, the unforeseen event would probably have added 30 minutes to the operation.

To exemplify the need for information, coordination, and revision of plans that could result from the unforeseen discovery of the lesion, we now expand on this simple but realistic scenario. While the events unfold, the *coordinator* will need to understand that the operation may be prolonged, and that the operating room may not be ready for the subsequent operation to start on time. The coordinator may need to find another *anaesthesiologist* to start the case in a neighbouring operating room, and the anaesthesiologist would need to be notified. The *recovery room* will need an update on when they can expect to receive the patient in order to manage their patients and resources and plan when to discharge patients to hospital wards in order to cope with the incoming flow of patients. The *assisting surgeon* may be scheduled to perform a case in a different operating room after the ongoing case, and the coordinator may need to find another surgeon for that case. When the patients' wife shows up at the ward, *the ward secretary* will need to know if the operation is finished and whether the patient is well. The delay may also cause the cancellation of a subsequent operation, in which case the *ward* needs to be informed so that they can notify the particular *patient* and the *patient's family*. Finally, *teams in all other operating rooms* would like to be kept updated on overall progress and whether emergency operations will cause other delays.

3. Information Granularity and Level of De-Identification

One strategy for supporting coordination in the above scenario is to visualize information about ongoing activities to the many different actors who need such insight. The involved actors will be in need for information about *patients* as well as information about the whereabouts of *their colleagues*. However, not all situations will require the display of fully identifying information. Sometimes the display of partly or fully de-identified information will suffice to support coordination and re-planning. Different situations will require the display of information at different levels of granularity. Figure 1 is a simple illustration of how information about a particular activity in a patient's health care trajectory can be presented at different levels of granularity and de-identification. This range of representations could simultaneously be visualized in a number of different locations and to a number of different actors, but at levels of granularity and de-identification that are tailored to the specific recipients' situation and needs.

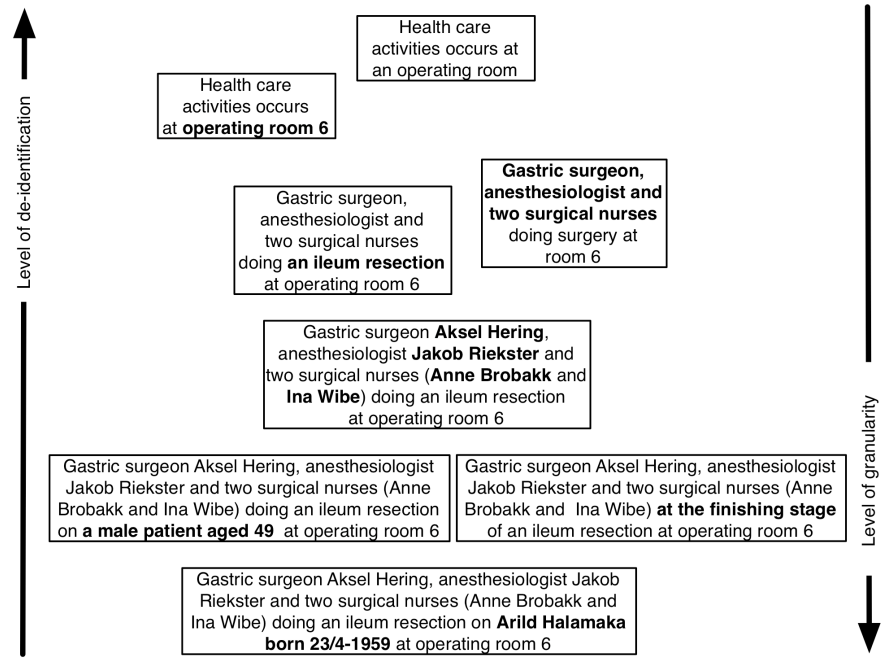

Figure 1. A tentative de-identification hierarchy for patient trajectories

4. Access Control and De-Identification/Privacy Challenges

The scenario presented here illustrates how information may be displayed simultaneously to many users in a collaborative environment for the benefit of improved cooperation and planning. In such a setting, privacy protection is a major concern. It is important to be able to protect the privacy of:

- The patient; the level of detail of clinical and identifying data should be kept at a minimum to minimize the risk of exposing sensitive information.
- The clinicians; the identity of those participating in the care of a patient may in itself be considered sensitive information, and visualizing the location of personnel may pose a threat to employee's privacy.

What information should be displayed depends on a number of factors, such as location, which actors that are present, what information the different actors need, and whom the information on display is about. The displays may be used in settings where only clinicians are present (e.g., team meetings) or settings where there is little or no control over who may be present (e.g., waiting rooms). Access policies are usually defined on a user level, and in a collaborative environment when all users present have the same view of information; the problem becomes one of policy combination. In general the principle of least privilege should be enforced [3], meaning that the persons with the least access rights will determine what information is available. This is good privacy-wise, but may result in a less usable system, as the clinicians with wider access

rights may not be able to see the information they need. One of the challenges we intend to solve as part of the COSTT project is that of combining access control policies. Access control policies will be specified per user type and situation based on studies observing clinicians at work in the hospital. Rules for policy combination will be created based on a trade-off between privacy needs and the need for information access. As shown in the scenario, the COSTT project will use flexible de-identification as an information security strategy, meaning that we will make information available at different levels of detail depending on the situation. The level of de-identification will be part of the necessary access control policies.

5. Discussion

The analysis of the scenario justifies the requirement that different actors will need different level of granularity of information richness. The solution requires a compromise between privacy demands and the need to know. During our research to develop a solution that meets these requirements, we will explore the following techniques: a) To reduce the level of granularity by de-coupling actor and role (e.g., replacing name of actor with name of role that the actor enacts), b) To de-identify by abstracting (e.g., replacing "patient with a tumour in ileum" with "patient with neoplastic disease"), c) To de-identify by replacing direct identifiers with pseudonyms, and d) By logging of individuals' as well as teams' use of information visualizations. The solution might require the implementation of technologies for location-based as well as proximity-based access control and might require the implementation of interaction techniques that differentiates between individual users' use of the system on behalf of themselves and on behalf of members of a team.

6. Conclusion and Future Work

The scenario and analysis presented here has been developed as part of the construction of a prototype that shall display representations of patient trajectories on wall-mounted boards. The system, that is to be developed iteratively, will first be tested with clinicians in a simulated clinical situation at our usability lab.

Acknowledgements. This work was supported by the Norwegian Research Council's VERDIKT program (grant nr. 187854/S10).

References

[1] Lenz, R., Reichert, M. (2007) IT support for healthcare processes – Premises, challenges, perspectives. *Data & Knowledge Engineering* 61:39–58.
[2] Strauss, A.L. (1997) *Social Organization of Medical Work*. Transaction Publishers, New Jersey, USA.
[3] Saltzer, J.H., Schroeder, M.D. (1975) The protection of information in computer systems. *Proceedings of IEEE* 63(9):1278–1308.