Healthcare professionals’ experiences with EHR-system access control mechanisms

Arild FAXVAAG\textsuperscript{a}, Trond S JOHANSEN\textsuperscript{a}, Vigdis HEIMLY\textsuperscript{b}, Line MELBY\textsuperscript{a} and Anders GRIMSMO\textsuperscript{a}

\textsuperscript{a} Norwegian EHR Research Centre, Faculty of Medicine, University of Science and Technology (NTNU), Trondheim, Norway

\textsuperscript{b} Department of Computer and Information Science, Faculty of Information Technology, Mathematics and Electrical Engineering, NTNU, Trondheim, Norway
introduction
• clinical work depends on access to relevant and updated information about the patient
• clinical work brings new information about the patient, to be stored in his/her record
• data are of very sensitive nature
• data must be made available to those providing care while at the same time kept protected from unauthorized access
privacy, information security and duty of secrecy

• three categories of subjects (with both rights and duties):
  – the patient, healthcare personnel and healthcare institutions
• two regulating regimes:
  – healthcare acts and regulations, personal data protection acts
• privacy is a right
  – both for patients and healthcare professionals
• healthcare institutions: duty to soundness, are responsible for the systems, shall maintain information security, shall perform information security audits
• healthcare professionals: duty of secrecy, duty of loyalty to employer
• patient: gives consent, principle of voluntary participation, right to participate in decision processes
duty of secrecy:

• norm for healthcare professionals regulated in law
  – differs from duty of secrecy outside the healthcare domain
• is related to that patients confess themselves to healthcare professionals
  – this gives “the narrowest possible mandate” to pass this information to others
  – and this means that the patient must give his consent if the information is to be used outside the original setting
• to acts and regulations, this means that:
  – relaying personal health data is seen as exceptions that must be regulated in law
  – this has brought complexity in laws and regulations
information security

• is about the duty of healthcare institutions to protect the personal health data they have collected from the patients

• about maintaining the availability, integrity and confidentiality of the data

• and about maintaining the view that all use of the information is a potential threat to information secrecy
  – access control mechanisms are mandatory
  – all use of the data shall be logged
an EHR system is also a tool for clinicians — has clinical purposes

Facilitate the clinical care of individual patients by:
- Assisting the health professional to structure his or her thoughts and make appropriate decisions
- Acting as an aide memoir for the health professional during subsequent consultations
- Making information available to others with access to the record system who are involved in the care of the same patient
- Providing information for inclusion in other documents (e.g. laboratory requests, referrals and medical reports)
- Storing information received from other parties or organisations (e.g. laboratory results and letters from specialists)
- Transfer the record to any NHS practice with which the patient subsequently registers (GP record)
- Providing information to patients about their health and health care

motivation for the study:

- details of access control mechanisms might impact the information seeking behavior of healthcare personnel
- little is known on how such mechanisms actually influences clinical work
- access control mechanisms might make access to relevant information more cumbersome and time consuming
- different methods of implementing information security policies might have different impacts on the users of the system
- how healthcare professionals perceive the use of access control mechanisms is largely not known
participants and method
• questionnaire with items related to
  – perceived use of time while presenting the user name and password to the access control component of the EHR-system
  – the effects of the automatic logoff mechanism
  – the impact of the access control mechanisms on how the respondents work with the patient’s EHR
participants

- clinicians at nursing homes:
  - 45 municipalities invited (one nursing home per municipality); 29 decided to participate; paper questionnaire distributed; 239 of 590 (41%) of the employees participated

- hospitals:
  - 21 hospitals / two departments per hospital
    - 1352 employees
    - leader of department contacted and asked to distribute a questback-based questionnaire to candidate respondents
    - 206 questionnaires (15%) were returned
results
• more than one out of three reported that the login routines often contributed to delays in their work.
• in nursing homes, 52% reported that the access control mechanisms had them relay messages about the patient orally rather than documenting in the patient’s EHR.
• Access control mechanisms also influenced on use of the EHR system for reading purposes.
• 46% of the respondents from the nursing homes reported that the logon procedure contributed to that they fail to look up in the patient’s EHR in advance of providing care to the patient.

• many reported that they often postponed documentation work until they could find the time to log on to the system.

• Among the hospital employees, 16% reported that documentation work always or often was done in the name of others
attitude to, and personal experiences with using access control mechanisms

- **First login takes too much time**
  - Hospitals (%): 17, 18, 2
  - Municipalities (%): 20, 18, 1

- **Every login takes too much time**
  - Hospitals (%): 15, 21, 2
  - Municipalities (%): 20, 20, 0

- **I often have to log other users off before I can login myself**
  - Hospitals (%): 11, 38, 5
  - Municipalities (%): 16, 47, 1

- **I rarely fail to log on to the system**
  - Hospitals (%): 12, 27, 1
  - Municipalities (%): 11, 32, 1

- **Automatic logoff happens too quick**
  - Hospitals (%): 22, 45, 4
  - Municipalities (%): 21, 59, 2
The patient's EHR is not checked before providing care to the patient

Messages are mediated through oral communication rather than via the EHR system

Work is delayed

Work is done on paper rather than with use of the EHR system

Documentation work is postponed until the personnel have time to document

Documentation work is done in the name of others

Effect on clinical work
interpretation
• today’s implementations of access control mechanism are perceived to have a negative impact on clinical work
• clinicians postpone documentation work
• access control mechanisms also alter their practice of reading what others have documented
relation to the setting of the work

**Work at the ward:**
- Laptops / mobile workstations mostly absent
- Many workstations in documentation room
- Many clinicians
- Many patients (in separate rooms)

**Consultation room: A traditional setting**
- One workstation
- One user
- One patient at the time
- Patient in same room as workstation
role of time constraints

• much of the work is done away from a workstation
• patients have conditions that require continuous attention and care
• spending time taking care of the patient must be prioritized
• from the perspective of clinicians, maneuvering through an access control mechanism takes time and therefore is perceived as having a cost
• some of the reported practices might be interpreted as workarounds, developed to accommodate their use of the EHR-system with other clinical tasks
patient safety issues

• delayed updates of the patient’s EHR, and preferring to share patient information through oral communication makes the information in the EHR less reliable

• not checking the patient’s EHR before providing care to the patient is a potentially dangerous practice
implications

• need for monitoring of unintended consequences
• need to improve access control mechanisms
  – are there usability issues?
• the value of access control mechanisms that take into account that healthcare institutions have zones with restricted physical access should be explored — i.e. that clinicians in close proximity of the patient should have a somewhat easier access to the patients’ data
• effect of equipping clinicians with a personal computing device (e.g. a iPad) should be explored
acknowledgements:

- Informants, participants in the advisory board, coauthors, Trond Henning, Arne Grimsmo

study conducted as part of “EPJ-monitor”, a survey of HIS system implementation of use in Norway

funding: The Norwegian Directorate of Health

contact info: arild.faxvaag@ntnu.no