When security prevents efficient work flow, users don’t follow security rules

Henriette Mabec*,

*Senior Research Associate, Ph.D Danish Institute for Health Services Research

Abstract

This case study exemplifies how end users disregard security rules in it systems. If security rules prevent efficient work flow, end users invent local work around practises that bypasses security rules build into it systems.

Results from this study are based on 200 hours of observations and 28 semi structured interviews.

The study shows that physicians and nurses don’t follow rules or act as intended in security matters, when security obstruct or delay patient treatment. Not even built-in security measures, as password and log on, force users to act as intended. They are loyal to the core value – patient treatment.

The study shows that there is a gap between theoretical security solutions, security solutions adapted from traditionally office work situations and medical practise. This calls for socio technical studies of medical practise, where users are observed in real life setting.

Keywords: Information science, medical informatics, medical order entry systems, medical record system, computer security.

Introduction

Data accessibility is one of the great benefits from computerized physician order entry system (CPOE), but accessibility also constitutes a potential risk of data falling into wrong hands because readers are innumerable when records can be accessed from everywhere [1:2]. To prevent misuse and to gain control, access to CPOE usually is restricted by mandatory use of user id and password.

In a socio technical point of view technology interacts with organisation. In this perspective CPOE isn’t 100% complete or finished when it is introduced. CPOE will modify and change in harmony with organizational task, culture, environment etc. [3]. Benefits related to it systems descend from the way organisations use CPOE. It is not the system, but the way users integrate the system in every day work situations that makes the difference [3].

The aim of this study was:

– to observe how users use CPOE

– to explore how users comply with security issues and rules

Before CPOE was introduced staff used a pen and their own initials to sign for an action. There were no identity control, and theoretically it was easy to cheat, if a person wanted to write wrong initials.

To prevent misuse and to gain control, CPOE is designed with access control consisting of unique user identification (log-in ID) and an access code (password). Both precautions are well known from offices and industries. This study reveals how clinical work and hospitals as work place differ from office work, and how this affect the effect from security precautions applied from office work.

Theoretical frame for understanding technology

This is a socio technical study, where technology is understood as a part of the organisation, where there is a mutual influence and interaction between technology and organisation [3-5]. This means:

– Technology acts differently in different settings

– Setting, task and the users affect technology in practise

In this perspective technology continues to develop in coherence with users. Technology makes network associations with other elements in clinical work practise [3,6-8]. This point of view implies that there is a possibility, that successful it solutions working in one situation can be a failure in another situation.

The study is inspired by Marc Berg, who has illuminated how the medical work situations differ from the normal office work place [9,10].

Materials and Methods

This is a case study carried out on a haematological ward and out patient clinic at a Danish University hospital [11-13].

The CPOE system was introduced one year before this study. To prevent misuse and control access to CPOE, the system was designed with unique user id and a personal password. These security precautions are well known from other computer systems. The idea is that the security precautions ensure that
only authorised persons can access confidential data, and that it is possible to identify and track who have gained access to patient data.

To study nurses and physicians working with CPOE ethnographic methods such as observations and interviews were used to enlighten real life situations and details in interaction between medical staff and CPOE [14-16].

The results are a part of a large research project with approx. 200 hours of observation and 28 semi structured interviews with nurses and physicians.

Observations were methodologically inspired by grounded theory going from rather open observations towards more focused observations [17,18].

There were two aims connected to the first observation round. The first aim was to explore variation in work. The second aim was to identify interesting situations for further investigation.

Following questions were used as an observational guide line:

- What happens? Description of situation and task
- Where? Description of location and organisation related to location e.g. room size, organisation, light, furniture etc.
- Who participates? Is one or more person engaged?

After the first round of observations, two situations were selected to further observation:

- Daily ward round
- Nurses preparing and distributing intravenous medication

The following semi structured interview focused on two themes:

- How do you use CPOE in your daily work?
- What changes in your daily work situation have you experienced in connection to the use of CPOE?

All observations and interviews were transcribed. After transcription the material was analysed and categorised. In the analytical phase of categorisation themes emerged from the material.

One of the themes was security and security issues coherent to organising work situation and location. This is the subject in this article.

Results

In this case study there were three situations where security related to user id and password was challenged:

1. When new employees or temporary workers haven’t got user id and password
2. At medication time when 4-5 nurses simultaneously need access to CPOE
3. When security rules prevent nurses giving medication

Example one: Users without user id and password

To use CPOE users need an account which is distributed by department of technology.

Observations and interviews reveal several situations where new employees or temporary workers didn’t have a user id and password, when they were on duty or began their employment.

The missing user id and password enforcing problems in the daily work flow, and secretaries are experiencing extra work load, when they try to solve the problem. Secretaries tell that they often phone or write more than once to the department of technology, when they haven’t got an account for new employees.

During the time of this study the problem with missing id and user accounts increases. It becomes more and more difficult for the department of technology to keep up with the numerous new employees and they lag behind creating accounts. After some time the hospital management gets involved. The chief physician of the hospital commands all physicians to pass their password and user id to colleagues who haven’t got a personal user id and password. The instruction letter from the chief physician of the hospital contains an additional instruction saying that all wards must create a manual list, where they register user identity and when who is who.

Example 2: Difficulties in access causes nurses share user id

At the ward the medication room is divided in two rooms. A big room used for tablet medication etc. and a small room used to prepare intravenous medicine. When CPOE was introduced there wasn’t finances to rebuild the medication room, and there wasn’t any table top to place a pc or a lap top in the little medication room. In the beginning nurses ran back and forth from one room to the other when they administrated intravenous medication. This wasn’t satisfying and after a while the local staff found a creative solution and placed a lap top in a storage cupboard, see figure 1.

![Figure 1: Lab top in medication room placed in cupboard](image)

For practical reasons nurses gives medication simultaneously to all patients. To keep continuation in the nurse patient relation, it is the assigned nurse who gives medication to patients who are assigned to her. This causes 4-5 nurses’ to have a need for accessing CPOE at the same time. The fact that there
is only one lap top and that the lap top is placed in a storage cupboard, makes it difficult to access CPOE when nurses has to register medication. The access problem increases at medication time, when several nurses need to access the system at the same time.

To save time the nurses have made an unspoken agreement: they use the same user id and don’t change user id between signing for medication. Observations show how first nurse in the medication room log on to CPOE. Afterwards the other nurses enter their actions in her user id. Nurses tell in the interview, that they are aware it’s wrong to share user id and password, but they argue that they don’t have time to change users. Nurses tell that they are aware of the risk of a reprimand, to which they expose them self, if another nurse gives wrong medication in their name. Some nurses tell that they try not to be the first to begin medication, because they don’t like it, when others register in their name.

At evening and night shifts the sharing of user id also is observed. The nurses tell that they know it is a bad habit, but explain or argue that they know and trust each other, when they are only two at a shift, and it is easier not to change users.

**Example 3: Security forces nurses to enter false signature**

Before CPOE nurses didn’t sign when they completed medication. CPOE demands monitoring every single action in medication, and nurses must sign when they complete medication. Further CPOE is provided with a security lock that prohibits new medication to be given, if previous medication isn’t completed in CPOE.

In the interviews nurses tell that they often have been in the situation, where they were to give medication, and the signature that illustrated completing earlier medication was missing, even though the task had been performed. Intravenous medication is given at the end of a duty, so when a nurse discovers a missing signature, the nurse who completed the medication has already left the ward.

The nurse who is to give new medication can choose between:
- making a false signature for an act she hasn’t done
- phone the nurse who forgot and try to force her to re-enter the hospital (maybe at 6 am)
- delay medication until to the nurse who forgot to sign are at work again

Observations and interviews confirm how nurses choose to sign for completion they haven’t performed. The CPOE offers no way to bypass request of signature in connection to completion before new medication can be given. If earlier medication isn’t completed, there isn’t any way to begin new medication.

**Discussion: User behaviour are based on values and can’t be controlled by it systems**

Examples from this study reveal how chief management and nurses prioritise efficiency in patient work above security solutions and administrative rules. There are three main problems connected to user id and password in CPOE:

1. **Built-in rules in CPOE are no guarantee if they don’t fit the local work practise**
2. **Security based on experience from office work can’t be applied to medicine without adaption and change**
3. **Rules without possibility to escape force cheating the system**

1. **Built-in rules in it are no guarantee, if they don’t fit the local work practise.**

Security precautions in CPOE descend from the idea that technology determines human actions. In contrast we find socio technical studies, where there is interaction and mutual dependency between technology and organisation. In this perspective technology changes and adapt to local environment [19-21].

This study illuminates the paradox that automatic control reduces security. Before CPOE there were nearly 100% similarity between signature and performing employee. Both the Danish National Board of Health and the Danish patients’ compliant commission verify this and tell that they have no knowledge of cases where staff deliberately has been using wrong initials. The authorities tell that there have been complaint situations where it has been difficult to read the signature, but no record of staff deliberately cheating.

This socio technical study shows how users adjust CPOE to make it fit daily work practise. Users don’t follow security rules in CPOE. Users act in accordance to values. When security rules disrupt efficiency or prevent actions related to patient work, the medical staff overrides security rules. Staff decides in the situation what is right and what is wrong to do in accordance to securing patient treatment and efficiency. The top management of the hospital also prioritises patient treatment and efficiency, when they legalise sharing of passwords and user id. The work load in the department of technology in connection to new employee was a surprise. The work flow analyses in connection to introducing CPOE concentrated on the clinician work and the impact in the clinicians’ workload, the deflected increased work load in department of technology was overlooked.

Security depends on interaction between users, environment, task etc. Users invent creative solutions and work around procedures that make them capable of overriding rigid rules, when they obstruct their main task. Designers of it systems hasn’t the power to decide the security level - not even by rigid rules. The level of security comes to life in connection with values, locations, organising work etc., when users use it systems.

In the end it is the end users, which have the ultimate power to decide security level in practise [3]. They decide when to follow or when to overrule built-in governed security [22-24]. Security can’t be decided by design of it systems.

This study illustrates how well known security solutions interacts with local work task and values. Local values transform, challenge and evolve security in daily work situations. There-
fore security must be evaluated by studies of real life situations and not by theoretical desk table calculations or laboratory test.

2. **Security based on experience from office work can’t be applied to medicine without adaption and change**

Office work differs from medical work. Usually office workers have a desk and a personal computer. They use the same pc during the day, and they log-on to their own pc in the morning and sign out when they leave in the afternoon.

Hospital staff move around different rooms and between wards. The staff use several computers during the day and share computers when working together.

The security system in CPOE is transferred from office solutions. According to Latour technologies are a result of negotiation [25]. In early stages technology is mutable, but slowly technology design and functionality become steady, and technology is taken for granted. At this time nobody questions the solution or think ‘it could be different’ [5].

User id and log on are reasonable security solutions, when employees have a desk and use the same and their own pc during a work day. In this study 4-5 nurses must share one pc at medication time, because of locations and work organisation. User id and password as security solutions were copied from the office work place without re-thinking security in connection to the organisation of medical work, hospital environment etc. User id and password as security control measures weren’t questioned. It was taken for granted that security precautions as user id and password would work without problems even when it was to be used in new settings and different situations.

This small study shows how security enters a broad network constituted from hidden values to more visible tings as hardware, locations etc. It was expected that the medical staff would use CPOE and log on as office employees, but organising work, culture, working conditions and values have shown a substantial influence on how users use CPOE.

Nurses and Physicians self-registration was suspended and replaced by automatic control which was transmitted from office work. When introducing CPOE there was a blind faith that technology determined solutions as compulsory user id and password were secure methods to control access. Lack of insight in difference between medical work and office work, and disregarding end users’ power to change technology lead to a practise that are more insecure than before.

The study indicates that managers and users in hospitals act according to the value of keeping production unaffected. If security rules constitute obstacles to patient work, users bypass the rules. The study enlightens that built-in security doesn’t determine the users way to interact with the system. End users are the ones who finally decide the security level, which can never be better than what the users decide. Therefore it is important to emphasise that security in health care it systems must be tested and evaluated in real life before implementing [26].

3. **Rules without possibility to escape force cheating the system**

The security rules in CPOE force nurses to make false registration, when they can’t begin medication. This wasn’t a problem before. If a nurse forgot to sign, the next nurse could perform her duties without any obstructions. The CPOE rules might be reasonable when designed theoretically, but developers and their advisers forgot the power, which was hidden in the imperfect human factor – nurses forget to register actions. Nurses fortunately act according to securing patients’ medication instead of following rules.

**Conclusion**

This small case study reveals how all organisational levels bypass security rules when security prevents efficient patient work. Users determine security in interactions between work, local environment and CPOE. Security solutions interact and evolve in use. It is the end users who decide when to follow the rules and when not to follow the rules.

Therefore security solutions from office work needs to be examined in real life situations before entering health care. Security solutions must not be transferred from one situation to another without being questioned and explored through socio technical studies of health care work. Further there is a need to explore what works before introducing it systems, so it systems doesn’t create security problems, that wasn’t a problem before CPOE.

**Acknowledgements**

Thanks to haematological ward Århus University Hospital, Managing physician dr.med. Jørgen Schøler Kristensen for permission to carry out the study. Thanks to Professor Christian Nøhr, Aalborg University and Professor Jes Søgaard, Danish Institute for Health Services Research for supervision throughout the project.
References

Reference List


Address for correspondence

Henriette Mabeck, senior research associate, Ph.D. Danish Institute Health Services Research, Dampfærgevej 27-29, 2100 Copenhagen Ø, Denmark.