Skyvell Nilsson *et al. Safety in Health* (2018) 4:11
https://doi.org/10.1186/s40886-018-0078-9

Safety in Health

RESEARCH ARTICLE Open Access

Professional culture, information security and healthcare quality—an interview study of physicians' and nurses' perspectives on value conflicts in the use of electronic medical records

Maria Skyvell Nilsson[1], Marianne Törner[2*] and Anders Pousette[2]

Abstract

Background: Digital healthcare information systems impose new demands on healthcare professionals, and information security rules may induce stressful value conflicts, which the professional culture may help professionals to handle.
The aim of the study was to elucidate physicians' and registered nurses' shared professional assumptions and values, grounded in their professional cultures, and how these assumptions and values explain and guide healthcare professionals' handling of value conflicts involving rules regulating the use of electronic medical records.

Methods: Healthcare professionals in five organisations in two Swedish healthcare regions were interviewed.

Results: The study identified ensuring the patients' physical health and well-being as the overarching value and a shared basic assumption among physicians and registered nurses. A range of essential professional and organisational values were identified to help attain this goal. In value conflicts, different values were weighted in relation to each other and to the electronic information security rules.

Conclusions: The results can be used to guide effective design and implementation of electronic medical records and information security regulations in healthcare.

Keywords: Healthcare quality, Organisational culture, Value conflicts, Information security, Rule compliance, Information management

Background

Web-based electronic medical records (EMRs) can improve healthcare by ensuring the completeness and coordination of patient information, but they also entail challenges to information security and to the quality of care. Information security is often defined by (a) confidentiality, i.e. that the information is available only to authorised individuals, units, or processes; (b) integrity, protecting the accuracy and completeness of the information; and (c) availability, i.e. that the information is accessible and usable on demand by authorised users. Information security is further defined by authenticity, accountability, non-repudiation and reliability [1].

EMRs facilitate availability but also imply new threats to information security. The electronic infrastructure makes patient data technically available to professionals who are not allowed such access. Access must therefore be regulated through rules. However, information security rules are not always heeded. They may pose ethical value conflicts when healthcare professionals must consider them in relation to other professional needs and values [2]. Value conflicts in healthcare commonly involve issues in which organisational demands are

* Correspondence: marianne.torner@amm.gu.se
[2]Occupational and Environmental Medicine, Institute of Medicine, Sahlgrenska Academy, University of Gothenburg, P.O. Box 414, SE 405 30 Gothenburg, Sweden
Full list of author information is available at the end of the article

perceived to conflict with healthcare staff's professional ethics. Ethical values are strongly related to the meaningfulness of work and therefore important for workers' psychological health [3]. Ethical dilemmas, which may cause moral distress, occur when health professionals are unable to adhere to their professional ethics [4] or know that acting on their professional ethics implies a breach of formal rules [5]. Kälvemark et al. defined moral distress in healthcare as 'traditional negative stress symptoms that occur due to situations that involve ethical dimensions and where the health care provider feels she/he is not able to preserve all interests and values at stake' [5]. A study among some 600 physicians and nurses found that moral distress was a problem in both professions and that there was a strong relation between moral distress and intention to leave the profession [6]. A literature survey showed that nurses who often felt moral distress were more emotionally exhausted and emotionally distanced from the patients [7]. These results indicate that moral distress caused by ethical dilemmas may not only jeopardise healthcare professionals' own health and pose a risk factor for exit, but that it may also induce a threat to the healthcare quality and patient safety. Organisational demands imposed by rules to ensure information security in the use of electronic information management systems are a possible source of ethical value conflicts in healthcare.

Johnson [8] stated that paradox or value conflicts in organisations could not be managed by prioritising one value before the other, since such values are interdependent. Consistently prioritising one value will increase the need for the other value. Coping with value conflicts may instead be facilitated by construing a perspective that accommodates opposing values. Such a framing of the value conflict allows a broader behavioural repertoire and active and flexible handling of paradoxical demands [9]. The organisational or professional culture may provide such a framing of value conflicts and thus help professionals to cope with them. Schneider and colleagues defined organisational culture as 'the shared values and basic assumptions that explain why organisations do what they do and focus on what they focus on; it exists at a fundamental, perhaps preconscious, level of awareness, is grounded in history and tradition and is a source of collective identity and commitment.' [10]. The culture thus provides a shared logic that sets limits for what may happen in the group, and if made visible, that logic may explain much of what happens. Professional culture is a concept related to organisational culture. Professional cultures often develop within communities with a long education and therefore a long period of professional socialisation [11]. In the medical and nursing professions, where the work is highly impregnated with emotions since it deals every day with issues of life and death, one may expect a particularly salient professional culture grounded in professional ethical values.

In one of the few empirical studies of professionals' perspectives on value conflicts in healthcare information security [12], Hedström and colleagues concluded that a control-based system would not work to introduce security procedures in an organisation where such value conflicts exist. To achieve better compliance with information security rules, the authors stated, one must study the meaning of what people say and do to better understand the interests and values that affect the practice of information security. Vaast [13] stated that information security issues are deeply embedded in the overall social and physical context of work and concluded that it is vital for security managers to get a grasp of these meanings to effectively design and implement security policies. We suggest that a cultural perspective on how value conflicts, involving information security in the use of EMRs in healthcare, are perceived and resolved may help to develop information security systems and policies that are better aligned with professional needs and thus better support the provision of high-quality, safe and efficient healthcare. Studying critical incidents in the work of healthcare professionals could illuminate cultural elements and explain behaviours within the professions. The present study aimed at elucidating physicians' and registered nurses' shared professional assumptions and values, grounded in their professional cultures, and how these assumptions and values explain and guide healthcare professionals' handling of value conflicts involving rules regulating the use of EMRs.

Methods

The present study was based on interviews in two phases. Phase 1 was performed to create the basis for phase 2, by describing common healthcare situations involving conflicts between information security rules and other professional values. The description of these situations was used as vignettes guiding the interviews in phase 2.

Participating organisations and context

The participating healthcare organisations were strategically selected to provide variation in location, size, medical specialty, digital software systems and organisation of EMRs. Swedish healthcare is organised into 21 geographic regions. Chief physicians in two caregiving organisations providing secondary and tertiary care in two such regions were contacted and agreed to participate. One region was represented by a university hospital organisation with two hospitals (310 and 673 beds) and the other region by three hospitals (498, 469 and 133 beds). Managers at the participating hospitals and units arranged contact with the interviewees, all of whom gave their informed consent to participate. All interviews were performed and recorded in secluded rooms at the participants' workplaces.

In phase 1, informants from the two participating regions, who upheld work tasks specifically related to the implementation of EMR systems, were purposefully selected to represent a variety of healthcare professionals and functions. The participants were well acquainted with different types of information security problems related to the use of EMRs. Two physicians, five nurses, two IT system developers and two healthcare managers ($n = 11$) were interviewed in phase 1.

In phase 2, new informants were selected. They were strategically selected registered nurses and physicians with varying degrees of experience and no specific responsibilities for implementing EMRs. They were selected from different medical specialties in hospital somatic and psychiatric care. Four physicians and four nurses from region 1 and three in each category from region 2 participated ($n = 14$). For more information about participants in phase 2, see Table 1.

Characteristics of the EMR systems in each participating region

In region 1, the Cosmic EMR system allowed all hospitals in the region, as well as publicly owned primary care and eldercare access to the EMRs. The access between organisations was limited to viewing, but not altering, information entered by another organisation. In region 2, the Melior EMR system served only hospitals and was not linked to primary healthcare EMRs. All hospitals in the region had viewing access to the EMRs.

Procedure and analysis

Phase 1

The semi-structured interviews in this phase, carried out in the spring of 2013, aimed to describe situations where value conflicts occurred in day-to-day work with EMRs. Sample questions were 'What are the information technology's main contributions to efficiency and quality of care?' and 'What obstacles do you perceive to the EMRs' ability to ensure information security?' The participants were e-mailed to collect their consent to participate and set times for the interviews. The interviews were recorded, and all expressions of values and basic assumptions related to information security were documented, coded and categorised. Situations in which healthcare professionals commonly experience value conflicts related to information security were identified and described. Based on this analysis, vignettes were constructed to illustrate 10 common day-to-day situations encountered by physicians or nurses and that represented dilemmas involving information security rules and professional needs to provide high-quality healthcare (see the Appendix for vignette examples).

Phase 2

The phase 2 interviews were performed from September 2013 to December 2014. Participants were asked to read the vignettes and select situations that were relevant and familiar to them. Each informant selected six to eight vignettes and for each vignette was asked to expand upon the following questions: 'How would you have acted in a situation like this?', 'What speaks for acting in such a way?' and 'What speaks against acting in such a way?' The participants were encouraged to reflect openly and to answer each question as completely as possible.

Table 1 Participants in phase 2 interviews

Geographical region	Professional position	Age (years)	Work experience (years)	Experience of EMR (years)	Professional specialty
I	Nurse	43	15	7	Internal medicine
I	Nurse	51	4	7	Surgery
I	Nurse	50	27	7	Surgery
I	Nurse	49	10	10	Psychiatric care
I	Physician	29	1	5	Surgery/orthopaedics//urology
I	Physician	32	5	5	Internal medicine
I	Physician	56	25	15	Orthopaedics
I	Physician	59	25	12	Psychiatric care
II	Nurse	49	26	6	Surgery; thorax
II	Nurse	47	10	5	Nephrology
II	Nurse	27	2	4	Nephrology
II	Physician	35	8	8	Surgery; urology
II	Physician	28	1	1	Surgery
II	Physician	48	22	13	Nephrology

The interviewer asked follow-up questions to induce participants to clarify or expand upon their answers. At the end of each interview, the participants were asked whether they could recall and describe any other relevant type of situation that would add further information.

A grounded theory methodology was applied to the data acquisition and analysis, providing a systematic, inductive and comparative approach to constructing theory [14]. The first step of the analysis was taken during data collection. After each interview, memos were created to record ideas about participants' values and assumptions about information security issues and their interrelationships. In this way, it was possible to continue to devise better-informed follow-up questions for the next interview and thus obtain a more detailed description of the phenomenon in focus. The interviews lasted 40 to 60 min, and recordings were transcribed verbatim (a total of about 200 pages of text). All authors read all transcripts. The first author was responsible for the primary analysis, but emerging results were discussed continually within the research team. When all interviews had been transcribed, we conducted a line-by-line coding of the text, which required close and repeated reading of the text. Meaning units, expressing values and basic assumptions related to information security were detected and coded. The next step of the analysis established the codes that best explained the empirical phenomena. Preliminary codes were tested against the text, and codes with the best 'carrying capacity' were distinguished [15]. A core category was constructed by pulling together tentative categories that explained this core category in a way that ensured theoretical significance and was traceable back through the data [16].

Results

The participants in the phase 2 interviews are presented in Table 1.

The analysis resulted in descriptions of one core category, four subcategories of professional values and three subcategories of internalised organisational value, and a theoretical model was constructed illustrating the interactions between these fundamental cultural elements (Fig. 1).

Ensuring the patients' physical health and well-being emerged as the core category, describing the common overarching value among the healthcare professionals. With this as a shared basic assumption, different internalised professional and organisational values and values underpinning prescribed information security rules were weighted relatively in the professionals' reasoning in decisions to act in dilemma situations. Such decisions were moderated by (a) assessments of the legitimacy of the information security rule(s); (b) situation-specific factors such as own competence, the competence of others

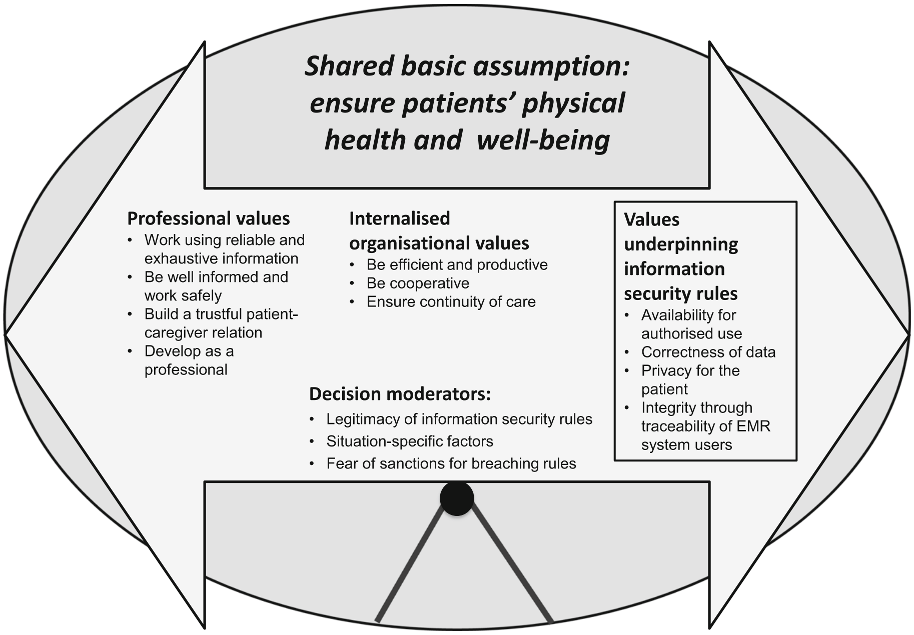
Shared basic assumption:
ensure patients' physical
health and well-being
Professional values
• Work using reliable and exhaustive information
• Be well informed and work safely
• Build a trustful patient-caregiver relation
• Develop as a professional
Internalised organisational values
• Be efficient and productive
• Be cooperative
• Ensure continuity of care
Values underpinning information security rules
• Availability for authorised use
• Correctness of data
• Privacy for the patient
• Integrity through traceability of EMR system users
Decision moderators:
• Legitimacy of information security rules
• Situation-specific factors
• Fear of sanctions for breaching rules

Fig. 1 The model illustrates the essential values among physicians and nurses, as they emerged in the study, and how different values are weighed in relation to each other, thus guiding adherence to formally prescribed information security rules. To keep an acceptable balance between different desirable phenomena (values and rules), the pivot point in the decision to act in a dilemma shifts dynamically, as the weight of each specific desirable depends on an evaluation of the entire situational context, and always in relation to the overarching value of ensuring the patients' physical health and well-being

involved and the patient's needs; and (c) the risk of sanctions if information security rules were breached. To balance the different values and rules acceptably, decisions on how to act in dilemma situations shifted dynamically, as the weight of each specific desirable depended on an evaluation of the entire context in each specific situation. The evaluations were always made to support the basic assumption that the highest value is to ensure the patients' physical health and well-being. Figure 1 presents a model of the results.

The resulting categories were persistently coherent between physicians and nurses and across specialties and organisations. Some differences between nurses' and physicians' professional roles could be discerned, however, as nurses stressed their coordinating function while physicians emphasised their medical function. Each quote below is marked with a code describing the informant's professional role of nurse (N) or physician (P).

The core category: ensuring patients' physical health and well-being

The overarching goal of healthcare emerged as protecting the physical health and well-being of the patients. Values that can ensure this overarching goal are protected, which may imply that information security rules are rated lower: 'The things that can kill you are more important than the ones that offend you.' (P)

Professional values

These values define what it means to act as a professional.

Work using reliable and exhaustive information

Reliable, relevant and complete information is considered a prerequisite to ensure patients' physical health and well-being. Completeness requires a clear division of responsibilities to secure the relevance and accuracy of the information as well as the rapid transfer of information between care professionals.

The information must be written distinctly and unambiguously. The patients' right to access their own medical records may then become a problem, since sensitive information such as unconfirmed or stigmatising suspicions can cause the patient anxiety and suffering. If such sensitive information has not yet been discussed with the patient, professionals may consider 'codifying' it. Patient privacy is thus weighted against the completeness, accuracy and lucidity of the text: 'It may be that the patient has access [to his/her electronic chart], so it's probably more important to express yourself in a way that is not hurtful.' (P)

Inadequacies in digital technology and software usability may also jeopardise information security. Accessing different types of patient information from different software applications requires the use of different computer display windows. The complete view of these is not as evident as it is in paper records, and some information may be unobserved. Also, multiple patient charts may be open on the computer simultaneously, which may cause confusion. Such inadequacies could cause healthcare professionals to base their decisions on incorrect or incomplete information. The source of the information must be possible to trace quickly and reliably, and EMRs do not always allow this.

Be well informed and work safely

Being well informed and working safely requires working conditions that allow professionals to summarise their observations and opinions and complete their documentation in peace and quiet. For example, physicians described that when they work in the emergency department, they do not always have enough time to ensure a well-informed decision. They therefore need to return to the information in the patient chart to come to more carefully considered opinions. Further, to gain an adequate summary of the patient's condition, a physician may also need access to medical records that are considered particularly sensitive, or even classified, such as those from psychiatric or gynaecological departments. The physicians also described that it may be difficult to specify in advance the information they need, as its significance may become clear only after a general search of the assessments and workups of other care providers. In some cases, no important information is gained from such searches and it may be difficult in retrospect to defend the decision to access the information. 'That's what you do to get a background of the patient's illness, so I don't just go into the internal medicine folder, but also the surgery folder and other folders that are necessary to get the patient's medical history.' (P)

Junior professionals may need to be advised in their medical decisions by more experienced colleagues. This may mean that the actual decision-maker is not documented in the EMR and traceability is compromised.

Build a trustful patient–caregiver relationship

Building and maintaining a trustful care relationship is a precondition of a healthcare professional's ability to provide, and the patients' ability to receive, appropriate care. To protect the relationship, it may be necessary to protect sensitive information from the patient's relatives. For example, if the information is considered highly significant, but the patient's consent to access it cannot be obtained without disclosing its existence to a relative, the healthcare professional may breach the access restriction. In such cases, the patient's approval is sometimes sought afterwards.

Patients' privacy rights may also conflict with protecting the relationship. A caregiving relation includes empathy and commitment, and professionals may consider it a human need to follow up on former patients to be updated on the patients' medical situation for a later appointment. This could mean breaching safety rules.

> Let us say that I have a patient with breast cancer that I may have followed now for two or three years. And then I get a mammogram report on her, let us say, and I write a reply and think 'Oh, how nice that this patient is doing well.' And then maybe I see in the surgery chart that the patient has presented as an emergency ... and has had surgery. And then there is great suspicion of relapse, and then I am like 'No, not her!' And maybe she's transferred to internal medicine, so we can do a work-up. Then I might go in and read the internal medicine chart because I want to see what's happening. It's wrong, I know it's wrong... It's about interest in how she's doing and for the future, because I might be seeing her at an appointment later. What happens then—should I call her? (N)

Develop as a professional

Healthcare professionals learn constantly through a variety of clinical situations and peer opinions. Such learning requires following up on patients and reading assessments from other caregivers after the care relationship has ended. Such access to information could conflict with information security rules.

> Why do I do it? To learn, so that I can become a better doctor for all of my future patients. I can understand that the patient does not want people to go in and read their charts. I agree with that... But, just for follow-up purposes, I think it's different... So it takes years before you become a good physician... And then I can make better decisions the next time I get exactly the same kind of patient. (P)

Internalised organisational values

These values related to being a responsible organisational team member and being efficient and productive.

Be efficient and productive

Maintaining care efficiency and productivity is integral to the professional role. This requires taking decisions and actions in complex situations where time is often limited, and it entails a need to prioritise tasks. Sometimes efficiency conflicts with information security. For example, patients in pain or who need their insulin must get medication immediately, but it is not always considered possible to document such measures at the time they are carried out, as required by the rules.

The professionals also described how conflicts between information security rules and efficiency could often arise through inadequate access to computers and inadequate usability, such as software that requires time-consuming management. Maintaining efficient care under such circumstances may compromise traceability in the EMRs. Poor usability also restricts the availability of the EMRs. Since using the EMR software can be complicated and time-consuming, it may be considered more efficient for the professional who is most experienced in such use to take care of the documentation. This can save time, but it compromises traceability.

The need to provide efficient care and ensure patient welfare implies that a patient should not be kept waiting for important drugs. Medication deemed necessary may then be administered by the nurse even if the prescription information in the EMR is incomplete. In such situations, the accuracy of the prescription is not checked with the responsible physician until afterwards, which poses a risk to both the patient and the nurse administering the drug.

> Yes, but you have to work pragmatically, I think, to work smoothly. You cannot just contact the on-call physician every time someone forgets to sign off on a prescription. That is not sustainable. (P)

In the absence of an EMR that is shared between caregiving organisations, physicians sometimes use a fax, order printed copies or make telephone calls to get up-to-date information from other healthcare providers. These procedures avoid delaying treatment decisions but jeopardise information security.

Be cooperative

Professionals cooperate to provide continuity of care, support each other, learn from one another and make use of each other's expertise. Collaboration is based on informal agreements on how medical care should be organised efficiently and on their shared responsibility to protect the patients' physical health and well-being. Such collaboration requires knowledge of each other's responsibilities and skills and functions as a control by which healthcare professionals can ensure that important interventions are carried out correctly and promptly. This includes warning others about any deviance from care procedures. For example, an experienced nurse who knows the procedures may remind the attending physician of a forgotten drug or question a prescription. Healthcare professionals described how the EMR software did not always support such cooperation, since it is not easy to follow interventions by those in other professional categories and how security rules sometimes have to be breached to ensure patients' health and well-being.

Collaboration creates opportunities to ensure and confirm the accuracy of personal actions. Less experienced physicians may need to consult experienced colleagues, who then need to log in to the patient's EMR without having a formal care relationship. Such log-ins may be frequent, and the reason for them is often not documented. Similarly, nurses described how they help each other with work on the ward, which entails reading the medical records of patients for whom they are not responsible. Further, treatment decisions are often taken in collaboration, where only the person who is logged in becomes formally responsible. Unclear delineation of what is authorised access to information does not support collaboration in healthcare, and the logs that are registered do not always mirror the actual work.

> It is unsustainable to work if we are not going to be able to help each other across boundaries when we need to do so. [...] If my colleague goes to the bathroom and the patient is doing poorly, then I get the care relationship. (N)

Ensure continuity of care

Healthcare professionals described having personal responsibility for maintaining continuity of care in patient transfers between different healthcare providers to avoid patients 'falling through the cracks'. They described following up on interventions and work-ups carried out at other healthcare facilities to ensure that planned and important problems and interventions were addressed. In some cases, such conduct is in conflict with EMR access rules.

> For me it's patient safety ... that what you ask for really gets done, that it will not be forgotten. It's happened when referring to a larger clinic that problems have been delayed which really need to be addressed faster... And I do not think it helps the patient in any way that I do not get to look. (P)

Healthcare professionals stated that the existing information technology systems cannot always ensure effective transfer of information and described how they use their own informal solutions to ensure continuity of care, such as a fax or hard copy chart passed along by the patient.

Decision moderators

Legitimacy of prescribed information security rules

Information security was generally considered a basic value in good healthcare, and the professionals were well aware of the information security rules. However, in their decisions on how to act, information security rules were weighted in relation to their legitimacy, to the professional's general attitudes toward regulatory compliance and to their interpretation of the concept of information security. However, violation of information security rules is legitimate only if based on professional needs, and there are clear limits to how far one may go in violating the rules.

> No, no. You cannot sign in using someone else's log-in. But on the other hand, [I] would spontaneously say she can check in on someone else's log-in, and then sign in afterwards using her own log-in. (P)

Various concepts in the information security regulations allowed some personal interpretation, related to the specific situation, individual role and professional needs.

> For me, the care relationship involves the patient that I am taking care of on this particular day. Or a patient who I have to call next week, when the patient and I have agreed to do so. That's how I see a care relationship. So, I hope that's right? (N)

Healthcare professionals said that patients are not aware of the limitations that apply to the professionals' access to patient information and that patients may not understand the medical consequences of personally restricting access to their EMRs. Healthcare professionals described ambiguities in individual assessments of how to handle restricted access and protected information: 'If they come to the emergency room, they want help; then I can break protection.' (P)

Nevertheless, restricted access imposed by the patient retains high legitimacy. Healthcare professionals described how they organise their work to try to follow the information security regulations. For example, one physician described how he, while the patient is still in the emergency room, asks for the patient's general consent to his accessing the chart notes later, to follow up on the case.

Fear of sanctions for breaching rules

Healthcare professionals described how it may be difficult to remember the reason for being logged on a specific patient. One physician described a need to 'look around' in different medical records to be able to analyse a patient's problems. Such an approach, which is intuitive and related to tacit knowledge, can be difficult to justify formally according to linear thinking. Another physician was concerned about breaking information security rules when consulted by other colleagues. In such consultations, physicians may access medical records without actually having any formal care relationship with the patients who are discussed. 'If they were to start asking, I couldn't answer why I was looking in the chart at the time. I didn't enter any documentation.' (P)

Discomfort with accountability also emerged in descriptions of how poor usability of the technology may result in accidental violations. For example, charts for different patients may be open on the computer at the same time, and the documentation could then be entered accidently on the wrong chart and/or by a non-authorised professional.

Traceability was perceived as both a threat to staff integrity and a means to ensure such integrity. It was considered a threat because of the risk of being accused of breaching the rules, because what is (un)authorised access to data was often unclear. However, it was also considered to protect the individual from being blamed for errors committed by others. Traceability enabled individuals to prove that they had met their obligations, if questioned.

Healthcare professionals also described behavioural circumventions and norms that support professional needs such as ensuring continuity of care or learning by accessing possibly restricted data but are not traceable. For example, the physician may read additional chart data while electronically signing a referral. This allows access to the medical records written by colleagues. Another example involves directly contacting the physician who took over the care of a patient with whom one's own care relationship has formally ended and asking questions. Such behaviour is considered acceptable, because the responding physician can sift through the information that is transferred.

> I would have called the surgeon who had received the referral and found out how the patient was doing through that channel... because then at least the surgeon would have an opportunity to say 'It's none of your business'. (N)

Situation-specific factors

A number of situation-specific factors were considered and influenced professionals' decisions to act. Examples of such factors were one's own competence, knowledge of the competence and trustworthiness of others involved in the situation, the urgency of the patient's needs and organisational and technical restrictions. Every decision was guided by the basic value of ensuring the patients' physical health and well-being.

> If I have known A for a long time, and I know that A is good and does not usually make any mistakes, I'd let A borrow my log-in. Of course, it depends on the patient. If it's a patient where it's important to administer insulin quickly, or if there usually is not any reason to hurry, that also makes a difference. That can always be evaluated. Obviously, it's the best interests of the patient that determine how you are going to act in a given situation. (P)

Discussion

Ensuring the patients' physical health and well-being emerged as the overarching value among physicians and nurses. We identified the need to satisfy this value as a shared basic assumption constituting the core of the professional culture [11]. In general, the professional and organisational values among nurses and physicians, and across organisations, were quite coherent. These findings support the existence of a largely shared professional culture, grounded in professional ethical values, and reaching beyond the organisational borders. The care of a patient often requires progression from one caregiver to another, within and between organisations. High-quality and efficient care then requires coordination between professionals, departments and organisations [17]. A shared professional culture is likely to facilitate this. Ensuring continuity of care also emerged as an internalised organisational value.

Information security was in accord with professional values such as ensuring patients' integrity and building a trustful relation with the patient. However, the EMR information security rules were considered too restrictive. This indicates that although the underlying values are coherent, the formal rules may cause stressful ethical dilemmas. Uncertainty about the interpretation of the rules, particularly regarding legitimate access to data, also posed problems for the care professionals.

Previous research on the pros and cons of introducing electronic information systems in healthcare have largely focused on the usability aspects of the technology, and recommendations to improve usability have been suggested [18, 19]. Healthcare professionals' concerns about their ability to use EMR technology illuminate the usability aspects of ease of use and interoperability and demonstrate that such aspects affect productivity, decision processes and individual priorities [20–23]. The present study also showed that EMR usability influenced users' reasoning and behaviour concerning compliance with information security rules. Although the optimal solution would be to eliminate all usability constraints, this is probably unrealistic due to differences between individual users and frequency of use, multiple systems in parallel use in different organisations, systems evolution with the integration of new subsystems and limited resources. Also, updates to information technology systems, even when they imply improvements, place an extra cognitive and emotional load on users. Usability aspects should be considered when developing information security procedures for the use of EMRs. But the present study widens the perspective beyond usability issues. It illuminates value conflicts in the use of EMRs and how such conflicts are handled within the professional culture in healthcare. This perspective is important because it may help healthcare managers and systems developers to understand why information security rules are sometimes breached and why coercive behavioural demands will not solve this. If they are not sensitive to important aspects of the professional culture, such demands may create ethical dilemmas that induce harmful moral distress. Information security rules and the organisation of work must accommodate a range of values essential to healthcare professionals' abilities to provide high-quality, safe and cost-effective healthcare.

The professionals described workarounds. They may ensure future access to information without breaking the information security rules by asking for the patient's general consent to do so. This may solve some concerns about the patient's autonomy, but it raises other ethical problems. For example, for how long is such consent considered valid? When is it right to ask such a question to a patient in need or dependency? The study also shows that there are several situations when it is not realistic to get consent from the patients, for example while cooperating with other professional team members or when a senior physician is consulted about a patient.

In line with other research [20], the participants described that the EMRs provide more complete documentation than analogous systems, but for some professionals and in specific situations, information security rules restrict the availability of the data in a way that is counter to high quality care. The study also showed how concerns such as the need to maintain a trustful relationship with the patient may compromise information security in terms of completeness, relevancy, and timeliness. Reliable and exhaustive information is crucial, but the professionals were concerned about the validity and quality of data in the EMRs, as has been found by others [24].

The information security rules themselves, or uncertainty about the interpretation of these rules, were found to restrict opportunities for professional development. Professionals may also need to access the patients' medical records after handing over the patient to other healthcare providers, to reflect on and learn from their own and other professionals' decisions. The professionals were uncertain about when such access to data was allowed under the information security rules. The Swedish Patient Data Act (SPDA) [25] in this respect is vague, and such ambiguity contributes to moral distress.

The professional values were essential for satisfying the basic shared assumption that the patients' physical health and well-being must be ensured. It is, however, interesting to note that important values were not grounded solely in professional ethics. Organisational values in terms of being efficient and cooperative were also highly internalised. The 'product' in healthcare work is care. The professionals are well aware that resources are sparse and must be used efficiently to accomplish high-quality care for all those who need it. Using resources in a careful manner is thus related to meaningfulness, role definition and cultural assumptions.

The results showed that healthcare professionals might sometimes breach information security rules to be able to cooperate and work efficiently. Prioritising cooperation among healthcare professionals at the cost of information security was also described in an observational study [26]. Such teamwork makes it possible to assimilate comprehensive competence and stimulates organisational learning [27].

In highly complex and varied work, such as healthcare, the rules regulating work performance must be formulated such that they allow professionals autonomy and adaptive behaviour in situations that cannot be well predefined [28]. It is important that when developing and implementing behavioural rules, processes and software, healthcare managers and designers of electronic information management systems acknowledge that information security is not a value that can be considered in isolation from other professional values in healthcare. Such recognition will allow the development of EMR systems that work in synergy with the professional ethics and culture. This would facilitate the healthcare professional's ability to accommodate different values and promote healthcare quality and performance, including a high level of information security.

Implications for practice

The need to ensure the patients' physical health and well-being emerged as a shared basic assumption within the professional cultures of physicians and nurses. A range of competing and sometimes conflicting values were considered in relation to this basic assumption and guided the professionals' decisions and actions. It is important that politicians, managers and others involved in organising and developing processes and procedures in healthcare understand and acknowledge this cultural assumption as an essential prerequisite for quality and equity in healthcare. Taking a stance on professional ethics in the design and implementation of new technology, such as EMR systems, and when developing rules regulating its use will allow professionals to accommodate a range of different values and improve their ability to cope effectively with value conflicts. Such alignment would not only reduce moral distress among the professionals, but also improve both healthcare quality and information security.

Limitations

The study was confined to two healthcare regions in Sweden, which may limit the transferability of its results. However, the differences between the EMR systems' design and organisation of data in the two regions contributed to descriptions of a variety of situations and thus to a deep understanding of the value categories and the reliability and exhaustiveness of the information. It should also be noted that the two different EMR software systems used in these two regions are commonly used in other Swedish healthcare regions. We also believe that most of the usability aspects of the electronic technology would be similar no matter the hardware or software used, since many design features are similar. Other studies focusing on users' behaviour and attitudes towards EMRs show that professionals in healthcare organisations in other countries have experiences similar to those described here [17, 23, 24, 26], which supports the transferability of our results.

In phase 2, the vignettes we used might have restricted the participants' responses. However, the vignettes were constructed to comprehensively represent the salient values and dilemmas described in the phase 1 interviews with participants with profound knowledge and experience of the problem area. The participants in phase 2 confirmed that the situations described in the vignettes were relevant to their day-to-day work. In addition, the phase 2 participants were given the opportunity during the interviews to describe other situations significant to the topic. No new categories emerged from their additional descriptions. The vignettes helped the informants to focus on realistic and common critical incidents and thus minimised the risk of stereotyped answers by reminding them of situations they had actually experienced. The open questions allowed us to acquire comprehensive descriptions of relevant phenomena.

According to grounded theory, a small number of participants could limit the theoretical saturation of the resulting categories [29]. In selecting participants, we sought as much variety as possible in the target population in terms of workplace, occupation, seniority, clinical specialty and geographical region. To ensure the saturation of the data, we returned to the two last analysed interviews and ascertained that no new categories had emerged in their analysis. We therefore consider the data exhaustive and thoroughly descriptive of the identified categories [30]. The results were fed back to and discussed with managers, IT system developers and healthcare professionals from the two participating healthcare organisations, some of whom had also been informants in the study. The results made sense to the feedback participants, which strengthens the validity of the results.

Conclusions

Ensuring patients' physical health and well-being emerged as the core category and shared basic assumption of the professional culture of physicians and nurses. The study also identified professional needs and values to ensure this basic assumption. Values underpinning information security rules were largely internalised, as were the organisational values of efficiency and cooperation. Although unproblematic when viewed individually, values sometimes came into conflict with the security rules regulating the use of EMRs. In such situations, values and rules were weighted dynamically in relation to each other in the professionals' normative reasoning and decisions on how to act to best satisfy the shared basic assumption. A range of situation-specific factors was then considered, along with the perceived legitimacy of the rules surrounding information security and the professionals' fear of sanctions if they breached those rules.

It is important in the development of EMR systems to view information security as one value among others, always in relation to the basic and shared assumption among the healthcare professionals, that first and foremost the physical health and well-being of the patient must be ensured. It is also important to work towards procedures and rules that can reconcile different needs and values, work in synergy with the professional culture and promote organisational performance. Such alignment will reduce value conflicts and moral distress among healthcare professionals and reduce the circumvention of information security rules.

Appendix

Examples of vignettes derived from phase 1 interviews and used in phase 2

1. Nurse A is handing out morning medications on the ward. One of the patients needs insulin before breakfast, so A is in a hurry. There is only one computer available in the medication room, and a colleague, who is also distributing medications, is logged in on that computer. A asks and receives permission to go into the patient's medication list via the colleague's login. Now the patient can receive the medicine on time, but A, who took out and administered the medication, will not be able to sign off on administering the medication.

What would you do in this situation, if you were A? What would you do if you were the colleague? What speaks for handling the situation in this way? What speaks against handling the situation in this way?

2. K works as a physician on the internal medicine ward. The day before yesterday, K met a patient with problems that K could not completely understand or solve. K believed that the patient's problems might have been surgical, so K referred the patient to the surgery department. Now K wants to follow up on this decision and see how things went for the patient. K goes into the surgery medical record system and finds that the patient was referred to gynaecology. Even more puzzled by the situation, K decides to read the chart note from gynaecology to gain clarity on the patient's problem. K logs in to the patient's gynaecology chart and reads it.

What would you do in this situation, if you were K? What speaks for handling the situation in this way? What speaks against handling the situation in this way?

Abbreviations
EMAs: Electronic medical records; SPDA: Swedish Patient Data Act

Acknowledgements
The study was financially supported by the Swedish Civil Contingencies Agency, grant no 2011-388, which is hereby gratefully acknowledged.

Funding
The study was financially supported by the Swedish Civil Contingencies Agency, grant no 2011-388.

Availability of data and materials
The datasets analysed in the current study are available from the corresponding author on reasonable request.

Authors' contributions
MT and MSN recruited participating organisations and healthcare professionals. MT, AP and MSN conceived and designed the study, developed the interview guide and participated in data analysis. MSN was primarily responsible for the data analysis and performed the literature review. MSN and MT wrote the first draft of the manuscript. All authors reviewed, discussed and edited the manuscript and approved the final version.

Ethics approval and consent to participate
The study did not collect information defined as sensitive by the Swedish Personal Data Act (i.e., data on race or ethnic origin, political opinions, religious or philosophical convictions, trade union membership, health, or sexuality) and therefore did not require approval from the Ethical Review Board. All participants gave their informed consent to participate in the study.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details
[1]Department of Health Sciences, University West, Trollhättan, Sweden.
[2]Occupational and Environmental Medicine, Institute of Medicine, Sahlgrenska Academy, University of Gothenburg, P.O. Box 414, SE 405 30 Gothenburg, Sweden.

Received: 21 August 2018 Accepted: 22 October 2018
Published online: 07 November 2018

References

1. ISO (The International Organization for Standardization) and IEC (the International Electrotechnical Commission). ISO/IEC 27002:2013. Information technology Security techniques Code of practice for information security management. Geneva. [cited 10 May 2018]. Avaliable from: http://docplayer.net/668061-Information-technology-security-techniques-code-of-practice-for-information-security-controls.html
2. Fernando JI, Dawson LL. The health information system security threat lifecycle: an informatics theory. Int J Med Inform. 2009;78(12):815–26.
3. Antonovsky A. Unraveling the mystery of health: how people manage stress and stay well. San Francisco: Jossey-bass; 1987.
4. Corley MC, Elswick RK, Gorman M, Clor T. Development and evaluation of a moral distress scale. J Adv Nurs. 2001;33(2):250–6.
5. Kälvemark S, Höglund AT, Hansson MG, Westerholm P, Arnetz B. Living with conflicts-ethical dilemmas and moral distress in the health care system. Soc Sci Med. 2004;58(6):1075–84.
6. Whitehead PB, Herbertson RK, Hamric AB, Epstein EG, Fisher JM. Moral distress among healthcare professionals: report of an institution-wide survey. J Nurs Scholarsh. 2015;47(2):117–25.
7. Oh Y, Gastmans C. Moral distress experienced by nurses: a quantitative literature review. Nurs Ethics. 2015;22(1):15–31.
8. Johnson B. Reflections: a perspective on paradox and its application to modern management. J Appl Behav Sci. 2014;50(2):206–12.
9. Lewis MW. Exploring paradox: toward a more comprehensive guide. Acad Manag Rev. 2000;25(4):760–76.
10. Schneider B, González-Romá V, Ostroff C, West MA. Organizational climate and culture: reflections on the history of the constructs in the Journal of Applied Psychology. J Appl Psychol. 2017;102(3):468.
11. Schein EH. Organizational culture and leadership. Third Edition ed. San Fransisco: Jossey-Bass; 2004.
12. Hedström K, Kolkowska E, Karlsson F, Allen JP. Value conflicts for information security management. J Strateg Inf Syst. 2011;20(4):373–84.
13. Vaast E. Danger is in the eye of the beholders: social representations of information systems security in healthcare. J Strateg Inf Syst. 2007;16(2):130–52.
14. Bryant A, Charmaz K. The SAGE handbook of grounded theory. Los Angeles: SAGE; 2010.
15. Charmaz K. Grounded theory as an emergent method. In: Hesse-Biber SN, Leavy P, editors. Handbook of emergent methods. New York; London: Guilford; 2008. p. 155–72.
16. Glaser BG, Strauss AL. The discovery of grounded theory : strategies for qualitative research. Chicago: Aldine; 1967.
17. Lluch M. Healthcare professionals' organisational barriers to health information technologies—a literature review. Int J Med Inform. 2011;80(12):849–62.
18. Fernández-Alemán JL, Sánchez-Henarejos A, Toval A, Sánchez-García AB, Hernández-Hernández I, Fernandez-Luque L. Analysis of health professional security behaviors in a real clinical setting: an empirical study. Int J Med Inform. 2015;84(6):454–67.
19. Lawler EK, Hedge A, Pavlovic-Veselinovic S. Cognitive ergonomics, socio-technical systems, and the impact of healthcare information technologies. Int J Ind Ergon. 2011;41(4):336–44.
20. Häyrinen K, Saranto K, Nykänen P. Definition, structure, content, use and impacts of electronic health records: a review of the research literature. Int J Med Inform. 2008;77(5):291–304.
21. McGinn CA, Grenier S, Duplantie J, Shaw N, Sicotte C, Mathieu L, et al. Comparison of user groups' perspectives of barriers and facilitators to implementing electronic health records: a systematic review. BMC Med. 2011;9:46.
22. Varpio L, Rashotte J, Day K, King J, Kuziemsky C, Parush A. The EHR and building the patient's story: a qualitative investigation of how EHR use obstructs a vital clinical activity. Int J Med Inform. 2015;84(12):1019–28.

23. Zwaanswijk M, Verheij RA, Wiesman FJ, Friele RD. Benefits and problems of electronic information exchange as perceived by health care professionals: an interview study. BMC Health Serv Res. 2011;11:256.
24. Salahuddin L, Ismail Z. Classification of antecedents towards safety use of health information technology: a systematic review. Int J Med Inform. 2015; 84(11):877–91.
25. The Swedish Patient data act (SOSFS 2008:355). [internet] Stockholm: Socialdepartementet [cited 10 May 2018]. Avaliable from: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355
26. Eikey EV, Murphy AR, Reddy MC, Xu H. Designing for privacy management in hospitals: understanding the gap between user activities and IT staff's understandings. Int J Med Inform. 2015;84(12):1065–75.
27. Skyvell Nilsson M, Pilhammar E. Professional approaches in clinical judgements among senior and junior doctors: implications for medical education. BMC medical education. 2009;9:25.
28. Grote G. Promoting safety by increasing uncertainty–implications for risk management. Saf Sci. 2015;71:71–9.
29. Charmaz K. Grounded theory: objectivist and constructivist methods. In: Denzin K, Lincoln Y, editors. Handbook of qualitative research. Thousand Oaks: Sage; 2000. p. 509–35.
30. Malterud K. Qualitative research: standards, challenges, and guidelines. Lancet. 2001;358(9280):483–8.