VIGILANT WORKING WITH IT AT SMALL MEDIUM ENTERPRISES IN HEALTHCARE

Student: Jesper Walinga
Student number: s2174014
University of Twente
Faculty of Science & Technology
Msc Health Sciences, 2024
Supervisors: dr.ir. A.A.M. Spil, dr. M. Renkema

Abstract

Background: Recent studies highlight that the lack of security and privacy policies disrupt healthcare operations, causing inefficiency and operational issues. Healthcare providers are mandated by laws like the GPDR to maintain the privacy, confidentiality, and security of patients' data, but caregivers' awareness may be insufficient. This research focuses on ECRs used for tracking the well-being of individuals. SMEs in healthcare struggle with cyber risks due to limited budget and staff. This research aims to define vigilant working and provide recommendations for SMEs to enhance employee awareness and organizational security. This research question contributes to literature and practice with a definition of vigilant working with ECRs, and eventually more secure, private, and safe SMEs in healthcare.

Method: This research used a mixed-method approach, combining a literature study with a case study. Using Wolfswinkel et al.'s grounded theory method, relevant topics for interviews were identified from the literature: Security, Privacy, Policy, Ethics, Trust, Confidentiality, and Safety. Semi-structured interviews were conducted with seven employees from WOPiT to explore these topics in a healthcare SME context. The interviews were recorded and transcribed, and that was followed by step-wise inductive coding, which identified eight themes.

Results: From the interviews, eight themes are determined. Security, Privacy, Trust, Policy, Data breach, Confidentiality, Ethics, and Safety. Participants acknowledge the importance of privacy and security, but the knowledge is often insufficient. The policy is not known thoroughly, particularly regarding data breaches. Employees maintain honesty with members in managing ECRs and confidentiality. WOPiT fosters a supportive environment where employees feel competent, trusted, and open to discussing issues, though there is room for improving knowledge.

Conclusion: Vigilant working should be defined as a way of handling patient's data where legal and organizational privacy, security, confidentiality, and ethical rules and procedures are taken into account. Despite recognizing the importance of privacy and security, employee knowledge on these topics is insufficient. Comprehensive policies, developed with a DPO, should be clearly outline duties, rights, and penalties. Strict access control measures must be implemented to prevent unauthorized access. Continuous and interactive employee training on privacy and security is essential, reinforced by occasional testing. Anonymization and pseudonymization techniques should be used to protect patient data. Transparency and honesty with patients build trust and enhance the work environment. By adapting and implementing these areas, SMEs like WOPiT can ensure the privacy and security of patient data while maintaining a supportive and open working environment.

Table of contents

Introduction

Recent studies have shown that the lack of standardized security and privacy policies have resulted in disruptions in healthcare [1]. These disruptions are for example, working inefficient, operational feasibility issues, and usability issues [2]. Laws and regulations, as the General Data Protection Regulation (GPDR) [3] force healthcare providers to keep patients' data private, confidential and secure. But the awareness of caregivers about, for example, the code of ethics, policies, laws and regulations may be not sufficient to maintain the integrity of the patients' data [4].
Knowledge and awareness in healthcare informatics, federal law and EHR data integrity will allow caregivers to provide advice to patients and other providers on best practices to maintain data integrity and build 'a safer system for better care' [5]. According to Platt et al. integrity, defined as honesty, captures confidence in upholding the principles of non-deception [6]. Ideally, healthcare allows for complete patient privacy as patients have the authority to allow or deny anyone to have access to their electronic health record (EHR) [1].

Electronic health records are online records where personal and clinical health-related information about a patient is stored [7]. EHRs improved healthcare in for example, fewer medication errors, improved clinical outcomes and data is more accessible. But there are also issues with the digitalization of patients' data related to integrity and patient safety [8]. For this research, the term electronic care record (ECR) is more suitable, because the scope of this research is on people with a psychiatric vulnerability who need a form of coaching or guidance. The coaching and or guidance is focused on, the individual not the psychiatric vulnerability, it is care instead of cure [9]. An EHR is more applicable in the cure-sector and an ECR is more applicable in the care sector [10,11]. The ECR is a record used to track the wellbeing and development of these persons and not only the medical status of the person.

SMEs in healthcare

Despite the growth of small and medium enterprises (SMEs) in Europe, innovative healthcare SMEs have struggled to get traction [12,13]. SMEs are enterprises with around, or less, than 50 employees [14]. Despite their economic importance, they seem to struggle with cyber risks. Limited budget and staff make it hard to mitigate those risks, as it is also not their core business [15,16]. Risk awareness and risk mitigation are important on an individual level as on an organizational level. Individual employees need to be made aware of the risks and how to mitigate risks, while on an organizational level it must be explained to the individual why and what must be and is done [13].

Mixing up terms like privacy and security is a common phenomenon [17]. Although these topics are intertwined, it is necessary to be able to keep them apart as well. This is hard, especially for SMEs where as said there is often not an expert employee for non-core business tasks [16].

In current literature, there is much information about topics as privacy, security, and policies on those topics, for example studies of Sahi et al. and Bani Issa et al. [1,5]. But the current literature fails to describe how SMEs, especially in healthcare, must handle working with their ECRs to make sure the information is private and secure, given their lower levels of budget and staff. To maintain security, privacy, and safety it is necessary to work vigilantly. Vigilance is defined as; *"more careful attention, especially in order to notice possible danger"* [18]. In literature, a fitting definition of vigilance in the context of this research is missing. Therefore, this research aims to investigate what vigilant working is, define what vigilant working with ECRs is, and how SMEs in healthcare can ensure vigilant working with ECRs whilst dealing with limited expertise and budget.

Research question

This leads to the following research question: *"How to ensure vigilant working with electronic care records at SMEs in care?"*

The goal of this research is to on one hand describe what vigilant working with ECRs is and on the other hand help SMEs in healthcare with recommendations on how to improve their employees' awareness and hereby keeping their organization safe and secure. Answering this research question contributes to literature with a definition of vigilant working with ECRs and how SMEs can ensure vigilant working. In practice, this will lead to more secure, private, and safe SMEs in healthcare.

Method

This research used a mixed-method approach consisting of a systematic literature study and a case study. First a literature study was conducted to identify relevant topics for the interview scheme and define vigilant working with ECRs. After that a case study, where semi-structured interviews were conducted, was performed to identify how these topics apply in an SME in healthcare.

Research design

For the literature study, the grounded theory method of Wolfswinkel et al. was used [19]. In Appendix 1 the search terms can be found in chronological order. Table 1 provides the search matrix in order of most topics discussed. The best search was: *care AND record AND privacy AND psych* AND trust*. This search had 36 hits and includes four articles that can be found in the search matrix. The other articles were found in an earlier search or with the back and forth referencing method [19]. Figure 1. displays the search process. Initially, six topics were identified through a thematic analysis [20]: security, privacy, policy, trust, confidentiality, and control. When delving deeper into the articles, ethics and safety were also identified as relevant topics. Control is removed as standalone topic, as access control is a major part of security. This made the final set of seven topics.

For the interviews, a case-study is performed. A case-study helps to delve deeper into a certain phenomenon, issues, and events in a real-life setting, as needed in this research [21]. Also, a case-study is useful attitudes and experiences with policies [21]. Through semi-structured interviews the view and knowledge of employees at a SME in care on privacy and security related topics, gathered from the literature study, were investigated. To ultimately answer the following research question: *"How to ensure vigilant working with electronic care records at SMEs in care?"*.

The Ethics Committee of the Faculty of Behavioural, Management and Social Sciences at the University of Twente has approved this research (application nr, 240431). Prior to the interviews, the participants were informed about the goal of this research, the duration of the interview and the use and storage of their personal data.

Article Topic	Security	Privacy	Policy	Ethics	Trust	Confidentiality	Safety
Bani Issa et al., 2020	X	X	X	X	X	X	X
Sahi et al., 2017	X	X	X		X		
Lee, 2017	X		X	X		X	
Platt et al., 2015	X	X			X		
Fernandez et al., 2013	X	X	X				
Blobel et al., 2017	X		X	X			
Benefield et al., 2006		X				X	X

Table 1. Search matrix

Interview framework

The topics from the literature study form the basis of the interview scheme, appendix 4. Per topic questions will be asked during the interviews. For security, privacy, and confidentiality, the study of Bani Issa et al. provides an example question. 'Based on your working experience, tell me about your concerns, if any, regarding the privacy of information in EHRs' [5]. Which is tailored to privacy, security, and confidentiality in daily practice for this interview scheme.
For the topic trust, the definitions of the four dimensions, fidelity, integrity, competency, and global trust are used to form questions [6]. For example competency, which refers to the ability and

expertise to minimize errors and achieve goals [6]. Which translates to the following question for the interview; 'Are you confident that you are doing your work well? (Minimize chances on errors?)'.
Furthermore, questions are asked to see if participants are familiar with the topics and how these topics come back in daily practice. For example, 'To what extent are you aware of the policy?'.
For the topic ethics an example situation is described, in which ethical considerations come into play. Questions about how the participant handles the situation and which considerations are taken into account are asked.

Figure 1. Display of Search Process

Research population

The participants for the interviews are recruited at Stichting Wonen en Psychiatrie in Twente (WOPiT) [22]. WOPiT is founded as a parent initiative for people with a psychiatric vulnerability. Since the start in 2006 WOPiT has grown to a SME in healthcare with six complexes and around 50 employees. The people with a psychiatric vulnerability live in one of the six small-scaled residential complexes. WOPiT also offers outpatient guidance. Everyone who is part of WOPiT, resident or employee, is seen as a member. In this way they strive for equality. Members live as far as possible independently in their homes in the residential complexes, with access to the communal facilities as the living room and garden. To create responsibility and autonomy the coaching is based on the member's initiative. The ECR that WOPiT uses is ONS of Nedap Healthcare [23].

The targeted participants were employees who are, recovery coaches/supervisors, recovery support worker, and office workers. These participants were recruited through quota sampling [24]. From all WOPiT's locations, including the office, one participant was recruited. The participants were included based on their employment status and their availability to facilitate a smooth data collection. The participants needed to sign the informed consent form (Appendix 2) to be included in this research, participants that did not sign the informed consent were excluded from this research.

The possible participants were contacted through an e-mail message. This e-mail message contained a brief explanation of this research, an information form (Appendix 3), the informed consent form (Appendix 2), and the invitation to participate in this research. If the targeted participant was positive about participating, an appointment for the interview was made by e-mail or phone. Eventually seven participants have participated in this research. Seven participants is considered sufficient, because the later interviews were not giving new insights, theoretical saturation was reached [25]. With signing the informed consent, the participant agreed to record the audio of the interview, and the use of the gathered data.

The gathered data was stored on the cloud of the University of Twente. The raw data was stored there until this research is finished and approved. After that, the data was destroyed. In the master thesis the data is not traceable to individual participants.

The characteristics of the participants are displayed in Table 2. The participants were all female, and the mean age was 40.9 with a standard deviation of 15,3.

Characteristics	Participants (N=7)
Age	40.9 (sd. = 15,3)
Female gender	7 (100%)
Education	Social Work (N=4), Applied Psychology, Nursing, Business Economics
Job	Recovery coach (N=6), Financial administrator
Work experience at WOPiT	1.7 years (sd. = 1,1)

Table 2. Demographics study population

Procedure

The interviews are based on voluntary participation and participants had the opportunity to end the interview at any moment and withdraw from this research. Consent to participate in the interview was obtained through the informed consent form (Appendix 2), in which participants also gave permission for audio recording. There were no risks associated with this research.

The interviews were conducted using a semi-structured interview scheme (Appendix 4), based on the topics from the literature study (*security, privacy, policy, ethics, trust, confidentiality, and safety*), and the analysis. These interviews were done on location. The interviews were semi-structured because following the interview scheme ensured that the interviews contained the same questions and had similar content, and it gave the opportunity to delve deeper into the topics when necessary. The topics are based on the literature search, see Table 1. In addition, demographic data (age, gender, job) were gathered.

Prior to the data collection the interview was reviewed by the deputy director at WOPiT and tested as pilot on a fellow student. This provided feedback to optimize the interviews and/or interview style before data collection. Before interviewing participants, the feedback on the interview style and brief explanation of certain topics had been processed.

Data analysis

The interviews were recorded with approval of the participant and were transcribed. For transcription the transcription function, and the dictation function of Word were used. The researcher improved the generated transcriptions. Names of participants were not used in this research; participants are referred as participant [A].

The transcripts were analyzed through stepwise inductive coding [26]. Open coding is the first step, the transcripts were divided into fragments and got a belonging code. There were 31 codes identified in this step. The next step is axial coding, during this step the made-up codes were being reviewed on describing the gathered data, the fragments were compared, and possible new codes were made. The initial 31 codes were brought down to 27 codes in this step. Lastly there is selective coding, this step gave further structure within the codes with the focus on answering the research questions [26]. In this last step the 27 codes were structured, and eight themes were identified in which the codes are displayed.

Initially, the topics from the literature study were disregarded while coding the interviews. These topics were the basis of the interview scheme, but while coding the interviews it became clear that the obtained knowledge from the literature study was used to code individual fragments and identify themes. There was one theme identified, that was not in the literature study. Other fragments and belonging codes were fitting within the topics derived from the literature study.

Literature study results

Security

Securing personal health information is crucial. According to Kruse et al. and Sahi et al. security has three pillars, access, administrative and physical safeguards [1,27].

1. *Technical safeguards* prevent or limit access to, in this case, digital personal health information and contain measures like data encryption [6], firewall [6], and access control.
2. *Physical safeguards* prevent or limit physical access to resources and contain measures like physical access control, workstation security, and assigned security responsibility.
3. *Administrative safeguards* contain measures that are both physical and technical, like risk analysis and management, having a Chief Information Security Officer (CISO), and system security evaluation.

There are concerns about unauthorized access to patient's data [5]. Who has access to what information, not every employee needs access to all patients but only their own [27]. Therefore, organizations should have clear policies on who has access to what information. Also, it means that security measures should be fitting per role in the organization [1].

Blobel et al. and Sahi et al. stated that communication and information security includes authentication on both ends of the line and accountability of principals involved, integrity, confidentiality and availability [1,28]. Without these principals privacy cannot be ensured and with the use of the three safeguards organizations gain patient's trust [1].

Every layer of an organization must be secure to limit security threats. Management must develop or follow strong policies on use of information, communication, and access control [1,29]. Furthermore, the most effective non-technical measures to promote security are education, training and awareness [7,29].

Privacy

According to Benefield et al. maintaining security is the first step to protecting patients' rights to privacy [30]. Privacy is the patient's personal right to have full control of their personal data according to Bani Issa et al. [5]. Lee defines privacy in a more extensive way as ''the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'' [7]. Sahi et al. defines privacy more precise and on the individual as: "Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data." [1].

Furthermore, privacy is also a more challenging issue and is seen as one of the biggest obstacles in healthcare due to the sensitive nature of the collected data and the data is not only of physiological nature but also habitual nature [1]. All clinical records must stick to the current law and regulations, but due to the fast development of EHR systems and changing laws and regulations, there are concerns about privacy [30]. Addressing these privacy concerns requires addressing the security safeguards. Pseudonymization, anonymization, and access control are ways to preserve privacy [1].

Privacy, and the feeling of privacy has a substantial influence on trust. Therefore, healthcare providers need to address these concerns with patients. In this way patients can understand how

their health information is used and negotiate the terms of such use [6]. This relates back to the definition of Sahi et al. with the individual's right to control their health information.

Health information is furthermore seen among the most confidential types of personal information. For maintaining privacy it is essential to protect this confidentiality [7].

Policy and standardization

To ensure that healthcare providers handle patients' data correctly policies need to be made. According to Blobel policies describe "the legal framework including rules, regulations and ethical aspects, the organizational and administrative framework, functionalities, claims and objectives, the principals involved, agreements, rights, duties, and penalties defined as well as the technological solution implemented for collecting, recording, processing and communicating data in information systems." [28].

Standards from the International Organization for Standardization (ISO) [31] and the Stichting Koninkrijk Nederlands Normalisatie Instituut (NEN) [32] can form the basis of these policies, especially the standards that are made specifically for healthcare [29]. Next to that constant users, healthcare providers, need to be involved when developing policies for EHR-usage to ensure that the policy reflects the best practice and preserves integrity [5]. Existing policies need to be evaluated in a continuous cycle to ensure that they still obey the current law and regulations and to limit the chances data breaches [1].

All employees of healthcare organizations should be trained and be aware of the importance of data security, along with an understanding of their and patient's rights and responsibilities in the context of privacy, confidentiality, integrity and availability of EHRs [1]. EHR policies and systems contain many techniques, including legal requirements, encryption, access control and logs in order to protect patients' data and maintain privacy [7].

Ethics

Healthcare providers should have ethical codes of conduct based on standards, for example set by the Internation Council of Nurses (ICN) [33]. These ethical codes clearly describe the ethical and legal obligations towards everyone involved in the healthcare process [5]. These codes of conduct, together with data protection legislation are a big component for access control in health information systems [28]. For ethical optimization of electronic health information data security is a necessity. The main risk of EHRs is that unintentional mismanagement will bring harm to individuals or communities [7].
Lee states that it is a professional's duty to investigate the benefits and minimize risks in working with EHRs based on ethical principles. If patients allow their EHR data to be used to benefit the care of others, then the minimalization of risks must be build-in [7].

Trust

One of the primary aspects of operational healthcare organizations is patient trust. As mentioned before, privacy is one of the biggest influences on winning trust in healthcare [1]. Trust is the basis of benefitting and secure handling of EHRs. Public trust is that the patients trust the caregiver to use the patient's data in a proper and secure manner. Trust is also trusting yourself and colleagues to use the patient's data in a proper and secure manner [5].

According to Platt et al. trust is defined as "a cognitive expectation or willingness to impart authority and accept vulnerability to another in the fulfillment of a given set of tasks. Trust contains four dimensions, fidelity, competency, integrity, and global trust [6].

According to Sahi et al. trust is intertwined with issues like confidentiality, integrity, accountability, authenticity, identity, and data management. To overcome trust issues, security and control measures must be taken, and patients must gain control over their personal health data, which complies to the definition of privacy [1]. Knowledge and privacy concerns are key factors in lower levels of trust. Trust may increase if someone is confident in the system's ability to protect their privacy. Furthermore, the quality, length and nature of the patient-provider relation has an effect on trust [6].

In policies, ways to effectively build or sustain trust should be described to develop patient-providers relationships, because no change may be the most risky proposition [6].

Confidentiality

According to Prater and Bani Issa et al. confidentiality is "an extension of privacy and mainly refers to protection of information, especially sensitive clinical information. Difference with privacy is there is an agreement or trusted communication between provider and patient." [5,34]. According to Sahi et al. confidentiality is "closely related to privacy and refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate."[1].

Patients may also request more confidential communication by designating a specific location be used for sharing and using of information [30]. As mentioned earlier health information is one of the most confidential types of personal information. Protecting this confidentiality is essential for privacy [7].

Safety

According to Virginio et al. safety refers to freedom from harm caused by medical management, as opposed to harm caused by the natural course of a patient's illness [35]. Factors that influence patients' safety in EHR context are interactions between the digital system and human-related factors, for example, typing errors. Maintaining patient safety is multifaceted procedure, that incorporates rules and addresses technological and non-technological factors [5].

According to Benefield et al. it may be the best practice for psychiatric patients to limit patient access to their EHR and provide patient access to their EHR when their mental health practitioner is available to provide support or answer questions [30].

Literature study analysis

From the literature, vigilant working with ECRs can be defined as; *"a way of handling ECRs where legal and organizational privacy, security, confidentiality, and ethical rules and procedures are taken into account."*

One thing that stands out from this literature study is that all topics are intertwined with each other, even more at SMEs [16]. As described, maintaining security is the first step to protecting privacy [30]. Whereas confidentiality is seen as an extension of privacy [5,34]. How to maintain security, privacy, and confidentiality should then be described and captured in the policy of the organization [28]. The

policy is also where the ethical codes of conduct should be addressed. Furthermore, privacy is a big influence on patient's trust [6]. Safety is a more separate topic in this case, which is more based on human or system's errors. How to handle such errors, as data breaches, should then be part of the policy. In short, it means that good and extensive policies should cover all these concepts for the organization. Covering all the concepts in the policy means; defining privacy, security, and confidentiality in a understandable way, describe what is covered by who, elaborate on what possible data breaches are, and how to handle them as an employee, and how the management team will handle these kind of situations, and explain the importance of vigilant working with ECRs [28].

Policies that are this extensive and well-written should provide transparency in the organization. When an organization is open and transparent, it is more likely to have trusty working environment. But, without sufficient knowledge on the topics described above, trust is more naivety or unjustified trust. Which allows privacy, and security risks into the organization. Therefore, the management should find a balance between trust and control.

The articles from the literature study mainly focus on bigger organizations, and mostly medical care. Whereas this research focuses on a small organization that provides coaching and guidance for people with psychiatric vulnerability. It is interesting to investigate if or to what extent these topics are of importance for smaller organizations. Ether way, there are several laws and regulations that need to be obeyed, such as, the GDPR and all employees sign a non-disclosure agreement [36]. Next to that, healthcare organizations in the Netherlands need to have a data protection officer (DPO) which helps and monitors the application and compliance of privacy legislation [37], which is hard for SMEs [38]. Using the specific expertise of a DPO is an opportunity for SMEs to develop their policy and organizational culture in the right secure way. Furthermore, the ISO and NEN provide standards about information security [39], but also standards specifically for healthcare like the NEN 7510 [40]. Furthermore, it is expected that trust plays a bigger role in SMEs and that policies are less extensive and less all-encompassing. In big organizations there is an expert-employee for everything and in small organizations employees are doing it on the side or as a part of the job [38].

Therefore, it is good to keep an eye on what is really required for a small organization to be working vigilant. Because they presumably do not have the workforce to cover everything into detail. It is worth looking at employees' knowledge and view on these topics and then see where the organization can improve, for example, their policy or personnel training.

Results

From the codes eight themes are determined. The eight themes are: Security (n=44), Privacy (n=39), Trust (n=35), Policy (n=32), Data breach (n=30), Confidentiality (n=11), Ethics (n=11), and Safety (n=11). Table 3 shows how often the themes have occurred in the data analysis. An overview of the themes with corresponding codes can be found in appendix 5. 'n' shows the number of fragments and 'N' shows how many participants have mentioned it. By using citates the themes are being described and possible differences within codes are being displayed.

Themes	Fragments (n=213)	Participants (N=7)
Security	44	7
Privacy	39	7
Trust	35	7
Policy	32	7
Data breach	30	7
Confidentiality	11	6
Ethics	11	6
Safety	11	6

Table 3. Overview themes

Security (n=44)

Within the theme 'Security' the following codes were identified: 'Technical safeguard' (n=19), 'Physical safeguard' (n=12), 'Concerns' (n=7), and 'Opinion' (n=6).

Technical safeguards that the participants mentioned were access control, secure mailing, 2-Factor authentication, and i-recognition. Within access control they mentioned the lack of access control in the old administrative system and that it is done well in the new administrative system. Secure mailing is their standard way of communication. 2-Factor authentication and i-recognition are needed to access certain programs.

"Especially with ONS later, that not all records are open access for everyone, unlike now." #ParticipantU.

Physical safeguards that the participants mentioned were locks and the shredder. Locks are used on every filing cabinet, laptops and the office get locked when they are left. The shredder is used after papers are digitalized.

"If we print something and do not use it anymore, we have to shred it. And to add, we have normal security here. Everything is locked … when nobody is in the office, lock the door." #ParticipantX.

The participants mentioned that overall they are not very concerned about the security. They mentioned that they are aware of security and that with ONS it only gets better. Although they do not say they do not make mistakes.

"I think we are doing pretty well. Yeah, sometimes someone will forget to lock a certain door, but that is sporadically." #ParticipantZ.

Also, the participants gave their opinion about security. They think it is sometimes cumbersome, but necessary.

"I think it is necessary. … I don't want my personal information on the streets, so I also don't want it for our members." #ParticipantY

Privacy (n=39)

Within the theme 'Privacy' the following codes were identified: 'Pseudonymization' (n=16), 'Awareness' (n=13), 'Opinion' (n=5), 'Concerns' (n=4), and 'Consent form' (n=1).

The participants mentioned that pseudonymization occurs when mentioning people in care records, in the incident reports, in the daily reports, on the planning board and in messages. Forms they use are, initials, descriptions, and (house) numbers instead of names.

"In the record, when talking about another person I use a description of that person, like upstairs or downstairs neighbor. That you don't use names explicitly." #ParticipantV.

Awareness is mentioned by all participants. They describe that they take into account where and when they have certain conversations with members.

"The mirrors of the office are taped off. But I notice that I want to double check sometimes, to see if someone is trying to hear the conversation." #ParticipantT.

Participants also gave their opinion about privacy measures. They all think it is a necessity because they also want privacy for themselves. But sometimes it feels like too much.

"It is a necessity, you don't want it for yourself and therefore also not for another" #ParticipantY.

"Once a colleague got sick, and they did not know where that colleague lived. So they asked for their address to send a card and flowers, but we are not allowed to give that. … I think that goes too far." #ParticipantW.

Participants had slight concerns about privacy. They said that you can not always protect privacy and had concerns about everyone's access to all records.

"You can't always protect members' privacy. They have things between themselves and that can be shared with others" #ParticipantY.

One participant mentioned that they use consent forms for special occasions.

"We had an audit a while ago … two members signed a consent form that their records can be used for the audit." #ParticipantW.

Trust (n=35)

Within the theme 'Trust' the following codes were identified: 'Colleague trust' (n=14), 'Competency' (n=14), and 'System trust' (n=7).

All participants described that they trust their colleagues and that it also the other way around. There is an open environment to give feedback on each other.

"Within the team we are critical, but not in a way that you feel attacked." #ParticipantX.

The participants are all confident that they do their job well. That confidence comes from experience and the collaboration with colleagues and members.

"I think what you get back from contact with members and colleagues … I feel my confidence growing." #ParticipantU.

The participants have system trust and think that the security and privacy regulations have a purpose for the system. However, not always necessarily for the care.

"That is a tricky question. Privacy is not always the best for care, but eventually it is for the system." #ParticipantV.

Policy (n=32)

Within the theme 'Policy' the following codes were identified: 'Handling' (n=11), 'Training period' (n=10), 'Knowledge' (n=6), and 'Recurring theme' (n=5).

The participants described their way of handling when not knowing the policy. At first, participants tended to ask the management team, but later they came back on that and mentioned asking their colleagues or looking into the manual as the first step.

"The step to the management team is not that big, so it is easy to ask them. But they will refer to the manual. … I think that I will check the manual myself at first." #ParticipantT

During the training period topics as vigilant working with IT are a part of the process, but the participants do not know if it is enough for everyone.

"Good, there was a training period checklist and buddy … but those topics could be a greater part. Due to staff shortage during my training period, it was a bit less." #ParticipantZ

The participants also made comments about their knowledge of the policy. They stated that they do not know the policy by hard but know where to find it.

"I know where to find the manual, but I have not looked it up lately." #ParticipantY.

If vigilant working with IT is a recurring theme depends per participant. It is not a recurring theme due to the management's actions, but by team's own criticism on each other. One thinks it is already such a part of WOPiT's culture that it is not necessary to make it a recurring theme.

"I don't think it is a recurring theme, I don't experience it that way. We are not reminded by the management team or anything like that." #ParticipantZ

Data breach (n=30)

Within the theme 'Data breach' the following codes were identified: 'Handling' (n=15), 'Meaning' (n=8), 'Policy' (n=6), and 'Opinion' (n=1).

The participants described how they would handle a situation where there is a data breach. At first, they would search for ways to undo it. After that, they would report it to the management team and both involved parties.

"You have to report it! … also report it to the person it's about and the person where the information does not belong to." #ParticipantW.

The participants also gave their meaning of a data breach. Which is, personal information that is shared with the wrong person/organization.

"I think information that is shared with the wrong persons and in particular sensitive information." #ParticipantT

Also, participants mentioned that they are not aware of the data breach policy of WOPiT.

"At this point, no totally not. It should be in the manual, but I haven't read it." #ParticipantX

One participant had a strong opinion about data breaches.

"When all big organizations, even the Pentagon, get hacked … how are we as a small organization supposed to prevent it." #ParticipantW

Confidentiality (n=11)

Within the theme 'Confidentiality' the following codes were identified: 'Honesty' (n=6) and 'Sharing at home' (n=5).

The participants mentioned that they are honest to the members. If members ask for something to be confidential, they will obey, but if that is not possible they will tell the member that they have to share it for certain reasons.

"In cases where a members does worrying statements and says I don't want you to anything with it. I know that colleagues are honest and say sorry I have to do something with it." #ParticipantT.

Also, the participants mentioned that sometimes they need to ventilate their experiences at home. Which is allowed, but not with names or any personal information.

"How do you handle it? Can I share with my partner? We talked about that with the team and agreed that you can share your experiences with your partner" #ParticipantY

Ethics (n=11)

Within the theme 'Ethics' the following code was identified: 'Handling' (n=11).

The participants described their way of handling a situation where ethical considerations come into play. A few mentioned there are signaling plans for every member to justify their actions. And they mentioned that in hindsight they will always discuss their handling with the member.

"Everyone has a signaling plan … these are the steps that we agreed on to take when the member is behaving like this." #ParticipantU

Safety (n=11)

Within the theme 'Safety' the following code was identified; 'Member access' (n=11).

The participants described their considerations about safety when the members get easier access with ONS. They will not twist the truth but have question if they should express thing differently.

"We discussed with colleagues yesterday … if they want to read it, it is okay. We maybe have to adapt another writing style, but never hide or twist the truth." #ParticipantU

Interview results analysis

From the interviews, it became clear that the discussed topics are intertwined with each other. As participants noticed that when, for example, they criticize each other on privacy-related issues working with ECRs, they are doing the same when it comes to security-related issues etcetera. Which means that trust, and the open working environment are important factors in vigilant working with ECRs at WOPiT.

WOPiT has a good, open, and transparent working environment, employees feel competent, trusted, and feel there is room to discuss things with colleagues and the management team. It is acknowledged that maintaining privacy and security is an important part of the job, as personal data, for an employee as well as a patient, must not be public. However, sometimes these measures are cumbersome, as it can feel like it is standing in the way of caregiving. And knowledge about privacy and security, and their additional measures seems not always sufficient. That knowledge can be improved by reading the manual/policy, as it is known where it can be found, but it is not read thoroughly. This lack of knowledge is also the case for data breaches. WOPiT has a policy in the manual, but it is not known by the employees, which can lead to handling data breaches wrong.

Also, in contact with members employees are honest in what they must share or note in the ECR. If the member asks for some things to be confidential, the employee is honest about if that is possible. WOPiT has made signaling plans for every member to capture what to do when a member is not approachable. Safety is a minor topic at WOPiT, which is mainly if they will change their way of administration if members have access to their record.

WOPiT has, and uses the knowledge of, a DPO and has the ISO 9001:2015 certification a standard for quality management with a focus on member and employee experience [41]. Also, there is an online manual where the ICT, GDPR, and data breach policy, among other things, can be found. Through the organizational structure with self-organizing teams, employees feel, and are trusted. But the management team needs to make sure that adequate knowledge is present.

In practice, how to obtain and maintain adequate knowledge should be captured in the policy of a SME. The application of this knowledge together with the open working environment, should validate trust.

Discussion

The goal of this research was to describe what vigilant working with ECRs is and on the other hand help SMEs in healthcare with recommendations on how to improve their employees' awareness and hereby keeping their organization safe and secure. From the interview analysis these eight themes emerged: Security, Privacy, Trust, Policy, Data breach, Confidentiality, Ethics, and Safety.

Key findings

From this research it is clear that all factors for vigilant working with ECRs are intertwined with each other. As mentioned in the literature analysis, that is even more the case in SMEs [16]. While performing the interviews this became even more clear. Therefore, it is suggested to make a careful explanation for privacy and security that fits the type and scope of the organization [17,42]. As these terms are often mixed up, due to their symbiotic nature [30]. According to J.J. Horning mixing up these terms is a common phenomenon, many people mean different things when using these words [17]. Also, knowledge about security and privacy seems limited. A fitting explanation, as mentioned above, should be in the policy together with all the rules, agreements, and procedures [28]. Therefore, employees should know what is in the policy. Now, employees are aware that the policy exists but not aware of the content while that is beneficial to mitigating security risks [43].

The procedures in the policy should describe how to maintain security and protect privacy by writing elaborately what employees' duties, rights and possible penalties are [28]. For example, what are an employee's duties and rights if a data breach occurs, and what are possible penalties. Next to that, it should be made clear what the employer, management team, does to support their employees to get adequate knowledge [1]. Adequate knowledge can be achieved during the training period and should be maintained by, for example, occasionally repeating tests [7,29]. Defining what this adequate knowledge is, and how to communicate that to the employees should be done in collaboration with the DPO. As the DPO is a helping hand for the application and compliance of privacy legislation [37]. As mentioned before, the specific expertise of a DPO is a major opportunity for SMEs to develop their policy and organizational culture in the right secure way.

From the interviews it became clear that access control is underdeveloped but improving. Access control plays an important in maintaining security [1,27]. The management team should prevent the possibility that employees have access to records of other patients than their own. This can, again, be done by developing strong policies on use of information, access control [1,7,29]. Per function in the organization, it should be described to which records, systems, and files access is required. If access is needed to another patient's record, it should be possible, but only with an explanation. In that way, the management can control if it was really necessary.

SMEs deal with similar security threats as large enterprises, but the budget constrain for SMEs makes it harder to deal with those threats. There is limited budget and expertise for adequate security policies, which makes SMEs an easier target [15]. Making a security policy that is in line with the type of organization, and making employees aware of that policy is the most important to manage risks [15,17].

Privacy at WOPiT is being preserved in the ECRs and collaborating systems through pseudonymization and anonymization. Names of members, employees, neighbors, and family members become initials, numbers, descriptions, and house numbers for example. The person's

identity is not directly known. This aligns with literature, pseudonymization and anonymization are common ways to preserve data privacy [1].

WOPiT's employees are very transparent and honest with their members. Which relates back to their identity and the open work environment [22]. This transparency leads to a more trusty environment with their members, but also between colleagues [6]. If possible, the employees communicate with the members what is done with their information. A lot of scenarios are talked through and a signaling plan is made for preventing and/or handling escalations [28]. In this way, they sealed the override of privacy laws and regulations as best as they could. And even after the escalations, the taken actions are evaluated within the team and also with the member in question. Although when asked about member access to the ECR, it became clear that employees change their mind a little bit. They will not twist the truth, but they might phrase it differently. G. Davidge et al. stated that there are some concerns regarding integrity and safety when patients have access to their personal records [30,44]. There are also potential benefits, which can be achieved with additional training and support [44].

Also, WOPiT's employees considered themselves competent in working with IT. That confidence mostly came from working with colleagues and members. Employees mentioned their satisfaction with WOPiT's open working environment where everyone is valued and approachable for criticism. Furthermore, the level of trust from and towards colleagues is very high because of the open environment. But because there seems limited knowledge about security, privacy, and related to pics, it is the question if they are doing well or are they not aware and therefore think that they are doing well. In short, is the trust justified? If this trust is based on affective trust, which is based on emotional ties between two, that does not say much about someone's capabilities. If this trust is based on cognitive trust, which is based on someone's integrity, competence, qualifications, and abilities, it is more justified [45]. During the training period, an employees' knowledge should be tested and/or trained. To finish the training period an adequate knowledge level should be required, as mentioned before. This adequate knowledge level ensures more cognitive trust. However, affective trust's importance can not be downplayed [46]. That is a big part of WOPiT's identity.

From the literature study and interviews, it appears that vigilant working is broader than just working with the ECR. Vigilant working with IT of digital vigilant working seems to be a more appropriate term. As mail, message applications, incident reports, daily reports, and other administrative systems for office workers also deal with patient's data and therefore need to be handled in a private and secure manner. Vigilant working with IT should be a dimension of vigilant working with patient's data as there is also a big physical part in maintaining security and privacy. For example, paperwork, planning boards, and locks on cabinets and doors. The definition for vigilant working with patient's data should be *"a way of handling patient's data where legal and organizational privacy, security, confidentiality, and ethical rules and procedures are taken into account."*

Limitations

One limitation of this research is that the participants' mean duration of stay at WOPiT is 1.7 years. This can be explained by the growth that WOPiT is experiencing. They hired a lot of new employees over the last couple of years. Interviewing more experienced employees could maybe give a better view on WOPiT's development of the policy, handling data breaches, training period now and then, and if security etcetera has been a recurring theme over the years.

Furthermore, during the interviews it became clear that the terms used were not always clear, or the participants were not familiar with it. This made it hard to answer the questions before these terms were explained. With sort of helping the participants, they gave useful answers. But maybe they were slightly steered towards those kind of answers by the explanation and examples. In hindsight, questions like, *What does … mean?*, should be asked to get insight in their knowledge and after that a given definition should be used during the rest of the interview. In that way, it should be clearer for the participant and the researcher.

Confidentiality as stand-alone topic was difficult to discuss as it is seen as an extension of privacy [5,34]. Participants struggled to properly answer the question, because they felt that it was a repetition of earlier asked questions. Confidentiality could have been a sub question of privacy, if participants did not mention confidentiality at all. And if they did mention confidentiality, it creates a more natural opportunity to delve deeper.

It was difficult to talk about concerns during the interviews. This expressed itself in two ways. One, they are convinced that they are it right and secondly their seemingly limited knowledge of the terms and topics. As mentioned earlier, this could be prevented by asking a knowledge question and after that work with a given definition.

After seven interviews with roughly the same tenor in terms of answers, theoretical saturation seems to be reached. Therefore, the results of this research are of use for WOPiT. However, the question is if this also applies for other SMEs in (psychiatric) healthcare. In further research, it is suggested to compare multiple SMEs to have a greater generalizability.

Recommendations

As mentioned before, in further research it is suggested to ask knowledge questions during the interviews, after researchers should work with a given definition of terms like privacy and security, and it is advised to compare multiple SMEs for generalizability.

Furthermore, it is recommended that the management team creates a policy with fitting definitions, description of procedures, raise awareness on these topics and this extensive fitting policy. This can be achieved by using the DPO's knowledge and expertise. The DPO can help finding a fitting definition, evaluating the policy, and recommend further steps [37]. It is also recommended to use data protection assessments (DPIA) when making decisions that involve high risk privacy issues. The DPO is obliged to give advice when performing a DPIA.

Having strict access control is recommended for SMEs. SMEs have a trusting nature, but there are employees that have unnecessary access to certain patient records. Access control is important for maintaining security, and proving that everything is done to maintain security [1,27]. It is advised to implement standardized strict access control.

During the training period it is recommended to include privacy and security issues in a way that employees know what it is and how to handle certain situations. It is recommended to provide clarity about the, for example, data breach procedures in the policy. Elaborate what employees' and employer's duties, rights, and possible penalties are [28]. That transparency should give employees the justified confidence that they know what to do in certain situations. Clarity creates unity in the way of handling. This can be achieved via an interactive training where definitions are learned and applied. After successfully finishing the training, the employee has the required knowledge to function well. This knowledge should be maintained over the duration of the contract, and therefore it is suggested to, for example, send fake phishing mails and/or occasionally repeating tests. When an employee clicks on the link in a fake mail, they are directed to a mandatory refresher course or something like that. This ensures that employees are keen on security threats and handle these situations in the right way.

For WOPiT it is recommended to develop their policy in collaboration with the DPO, implement standardized access control, train their employees to work vigilant with IT, and keep their trusty, and open working environment. In this way, WOPiT can ensure privacy and security.

Conclusion

The goal of this research was to answer the following research question: *"How to ensure vigilant working with electronic care records at SMEs in care"*. To understand what, and how to, ensure vigilant working, eight themes were identified: Security, Privacy, Trust, Policy, Data breach, Confidentiality, Ethics, and Safety.

Privacy and security are acknowledged as an important part of the job. However, knowledge about this topics is seemingly insufficient. A clear understanding is essential. Improved knowledge benefits the justification of trusting yourself, as an employee, and your colleagues. Through comprehensive policies that include fitting explanations and detailed procedures. Policies should outline an employee's duties, rights, and potential penalties. The policy should be developed with the expertise of a DPO. Whilst WOPiT is a well-performing SME, it still has limited expertise and budget to manage these issues, which is the main difference in comparison with bigger organizations. A DPO can provide the required assistance for SMEs, because the DPO is already familiar with the organization as a healthcare organization is obliged to have a DPO.

The importance of access control is currently overlooked in SMEs. Implementing strict and standardized access control measures is necessary to prevent unauthorized access. This includes defining access requirements per function in the organization.

Employee training is critical. Employees should be trained on privacy, security, and the policy during the training period and continuously through their contract at the organization. This training should include interactive elements. Occasional testing should maintain knowledge and awareness. Fake phishing mails can reinforce these practices.

Moreover, anonymization and pseudonymization techniques should be applied to protect patient data. Transparency and honesty with patient about their data builds trust and improves the overall work environment.

For SMEs, like WOPiT, to work vigilantly with ECRs need to:

1. Develop clear and comprehensive policies with the assistance of a DPO.
2. Implement standardized and strict access control measures.
3. Provide thorough and ongoing training for employees on privacy and security issues.
4. Foster a transparent and trusting work environment

If these things are adopted and implemented, SMEs can ensure the privacy and security of patient data while maintaining a supportive and open culture at work.

Reference list

[1] Sahi MA, Abbas H, Saleem K, Yang X, Derhab A, Orgun MA, et al. Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. IEEE Access 2017;6:464–78. https://doi.org/10.1109/ACCESS.2017.2767561.

[2] Parks R, Xu H, Chu CH, Lowry PB. Examining the intended and unintended consequences of organisational privacy safeguards. Eur J Inf Syst 2017;26:37–65. https://doi.org/10.1057/s41303-016-0001-6.

[3] EU. General Data Protection Regulation. Off J Eur Union 2016.

[4] LaMonica HM, Roberts AE, Lee GY, Davenport TA, Hickie IB. Privacy Practices of Health Information Technologies: Privacy Policy Risk Assessment Study and Proposed Guidelines. J Med Internet Res 2021;23:e26317. https://doi.org/10.2196/26317.

[5] Bani Issa W, Al Akour I, Ibrahim A, Almarzouqi A, Abbas S, Hisham F, et al. Privacy, confidentiality, security and patient safety concerns about electronic health records. Int Nurs Rev 2020;67:218–30. https://doi.org/10.1111/inr.12585.

[6] Platt J, Kardia S. Public trust in health information sharing: Implications for biobanking and electronic health record systems. J Pers Med 2015;5:3–21. https://doi.org/10.3390/jpm5010003.

[7] Lee LM. Ethics and subsequent use of electronic health record data. J Biomed Inform 2017;71:143–6. https://doi.org/10.1016/j.jbi.2017.05.022.

[8] Alpert J. The electronic medical record in 2016: Advantages and disadvantages. Digit Med 2016;2:48. https://doi.org/10.4103/2226-8561.189504.

[9] Choudhury D, Nortjé N. The Hidden Curriculum and Integrating Cure- and Care-Based Approaches to Medicine. HEC Forum 2022;34:41–53. https://doi.org/10.1007/s10730-020-09424-6.

[10] Cliendo. ECD: Elektronisch Clienten Dossier n.d. https://www.cliendo.nl/ecd-elektronisch-clienten-dossier/ (accessed June 4, 2024).

[11] Nedap Healthcare. Wat en voor wie is een elektronisch cliënten dossier (ECD)? 2021. https://nedap-healthcare.com/ons-home/nieuws-ecd/ (accessed June 4, 2024).

[12] Horgan D, Van Kranen HJ, Morré SA. Optimising SME Potential in Modern Healthcare Systems: Challenges, Opportunities and Policy Recommendations. Public Health Genomics 2019;21:1–17. https://doi.org/10.1159/000492809.

[13] Pickering B, Boletsis C, Halvorsrud R, Phillips S, Surridge M. It's Not My Problem: How Healthcare Models Relate to SME Cybersecurity Awareness. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12788 LNCS, 2021, p. 337–52. https://doi.org/10.1007/978-3-030-77392-2_22.

[14] Dobre O. Differences of Organizational Culture between Small and Large Enterprises. Ovidius Univ Ann Econ Sci Ser 2016;XVI:296–301.

[15] Khan MI, Tanwar S, Rana A. The Need for Information Security Management for SMEs. 2020 9th Int. Conf. Syst. Model. Adv. Res. Trends, 2020, p. 328–32. https://doi.org/10.1109/SMART50582.2020.9337108.

[16] Khurat A, Abendroth J, Bracher S, Krishnan P. Towards client privacy policy enforcement for small-medium enterprises. Proc. 2007 Inaug. IEEE-IES Digit. Ecosyst. Technol. Conf. DEST 2007, 2007, p. 319–24. https://doi.org/10.1109/DEST.2007.371991.

[17] Debenham J, Wagner RR. Protecting persons while protecting the people. vol. 3588. 2005.

[18] Cambridge English Corpus. Cambridge English Dictionary. n.d.

[19] Wolfswinkel JF, Furtmueller E, Wilderom CPM. Using grounded theory as a method for rigorously reviewing literature. Eur J Inf Syst 2013;22:45–55. https://doi.org/10.1057/ejis.2011.51.

[20] Sovacool BK, Iskandarova M, Hall J. Industrializing theories: A thematic analysis of conceptual frameworks and typologies for industrial sociotechnical change in a low-carbon future. Energy Res Soc Sci 2023;97:102954. https://doi.org/https://doi.org/10.1016/j.erss.2023.102954.

[21] Crowe S, Cresswell K, Robertson A, Huby G, Avery A, Sheikh A. The case study approach. BMC Med Res Methodol 2011;11:100. https://doi.org/10.1186/1471-2288-11-100.
[22] Stichting WOPiT n.d. https://wopit.nl/ (accessed May 2, 2024).
[23] Nedap Healthcare. ONS 2014. https://nedap-healthcare.com/oplossingen/ons/ (accessed March 11, 2024).
[24] Yang K, Banamah A. Quota Sampling as an Alternative to Probability Sampling? An Experimental Study. Sociol Res Online 2014;19:56–66. https://doi.org/10.5153/sro.3199.
[25] Guest G, Bunce A, Johnson L. How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. Field Methods 2006;18:59–82. https://doi.org/10.1177/1525822X05279903.
[26] Boeije H. Stappenplan kwalitatief onderzoek. Anal. kwalitatief Onderz., Amsterdam: Boom Onderwijs; 2005.
[27] Kruse CS, Smith B, Vanderlinden H, Nealand A. Security Techniques for the Electronic Health Records. J Med Syst 2017;41:127. https://doi.org/10.1007/s10916-017-0778-4.
[28] Blobel B. Trustworthiness in Distributed Electronic Healthcare Records - Basis for Shared Care. Angew Chemie Int Ed 6(11), 951–952 2017;9:5–24.
[29] Fernández-Alemán JL, Señor IC, Lozoya P ángel O, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform 2013;46:541–62. https://doi.org/10.1016/j.jbi.2012.12.003.
[30] Benefield H, Ashkanazi G, Rozensky RH. Communication and records: HIPPA issues when working in health care settings. Prof Psychol Res Pract 2006;37:273–7. https://doi.org/10.1037/0735-7028.37.3.273.
[31] ISO. International Organization for Standardization n.d. https://www.iso.org/home.html (accessed May 13, 2024).
[32] NEN. Stichting Koninklijk Nederlands Normalisatie Instituut n.d. https://www.nen.nl/over-nen (accessed May 13, 2024).
[33] ICN. International Council of Nurses n.d. https://www.icn.ch/ (accessed May 13, 2024).
[34] Prater VS. Confidentiality, privacy and security of health information: Balancing interests. Biomed Heal Inf Sci 2014. https://healthinformatics.uic.edu/blog/confidentiality-privacy-and-security-of-health-information-balancing-interests/ (accessed April 14, 2024).
[35] Virginio LAJ, Ricarte ILM. Identification of Patient Safety Risks Associated with Electronic Health Records: A Software Quality Perspective. Stud Health Technol Inform 2015;216:55–9.
[36] KVK. Confidentiality statement n.d. https://business.gov.nl/running-your-business/products-and-services/protecting-your-product-idea-or-innovation/confidentiality-statement/ (accessed June 7, 2024).
[37] Autoriteit Persoonsgegevens. FG-informatie 2024. https://www.autoriteitpersoonsgegevens.nl/fg-informatie (accessed March 4, 2024).
[38] Jantti M. Studying Data Privacy Management in Small and Medium-Sized IT Companies. Proc. 2020 14th Int. Conf. Innov. Inf. Technol. IIT 2020, 2020, p. 57–62. https://doi.org/10.1109/IIT50501.2020.9299050.
[39] ISO. ISO/IEC 27001:2022. 2022.
[40] NEN. NEN 7510: Informatiebeveiliging in de zorg n.d. https://www.nen.nl/zorg-welzijn/ict-in-de-zorg/informatiebeveiliging-in-de-zorg (accessed April 4, 2024).
[41] WOPiT. Bestuursverslag 2021:1–15.
[42] Ware WH. Security and privacy: Similarities and differences. AFIPS Conf Proc - 1967 Spring Jt Comput Conf AFIPS 1967 1967:287–90. https://doi.org/10.1145/1465482.1465525.
[43] Li L, He W, Xu L, Ash I, Anwar M, Yuan X. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. Int J Inf Manage 2019;45:13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.
[44] Davidge G, Brown L, Lyons M, Blease C, French D, van Staa T, et al. Primary care staff's views and experience of patients' online access to their electronic health record: a qualitative exploration. Br J Gen Pract J R Coll Gen Pract 2023;73:e418–26.

https://doi.org/10.3399/BJGP.2022.0436.
[45] Zhu W, Newman A, Miao Q, Hooke A. Revisiting the mediating role of trust in transformational leadership effects: Do different types of trust make a difference? Leadersh Q 2013;24:94–105. https://doi.org/https://doi.org/10.1016/j.leaqua.2012.08.004.
[46] Kim S, Lee C. Study Examines Role of Collaboration-Enhancing Factors in Supply Chain. Oper Supply Chain Manag 2024;17:77–88. https://doi.org/10.31387/oscm0560415.

Appendix

Appendix 1. Search logbook literature study

Search terms	Results	Valuable?	Search
care AND record AND privacy AND communication AND psych*	116	Yes	1
care AND record AND privacy AND communication AND psych* AND outpatient	12	No	2
care AND record AND privacy AND internal AND communication AND psych*	4	No	3
care AND record AND privacy AND communication AND psych* AND independent AND living	0	No	4
care AND record AND privacy AND communication AND psych* AND independent	3	No	5
care AND record AND privacy AND sharing AND psych*	48	Yes	6
care AND record AND security AND sharing AND psych*	21	No	7
care AND record AND security AND communication AND psych*	83	Yes	8
care AND record AND security AND communication AND psych* AND independent AND living	0	No	9
care AND record AND security AND communication AND psych* AND outpatient	7	No	10
care AND record AND security AND psych* AND outpatient	27	No	11
care AND record AND privacy AND communication AND psych* AND security	28	No	12
care AND record AND privacy AND communication AND psych* AND safety	14	No	13
care AND record AND privacy AND communication AND psych* AND trust	16	Yes	14
care AND record AND privacy AND psych* AND trust	36	Yes	15
care AND record AND privacy AND psych* AND control	58	Yes	16
care AND record AND privacy AND communication AND psych* AND control	26	Yes	17

Appendix 2. Informed consent

Consent form for interview – Master Thesis

YOU WILL RECEIVE A COPY OF THIS SIGNED CONSENT FORM

You are kindly invited to participate in an interview as part of my master thesis at WOPiT. Before you decide whether to participate, it is important to understand why the research is being conducted and what it entails. Please take the time to carefully read the following information before deciding to participate and consult with others if desired.

ABOUT THE RESEARCH

This research is conducted by Jesper Walinga under the supervision of dr. ir. Ton Spil from the Faculty of Behavioural Management and Socials Sciences and Industrial Engineering & Business Information Systems at the University of Twente. The aim of this research is to map out the knowledge and views on privacy and data security within WOPiT. The research has been approved by the Ethics Committee of HSS at the University of Twente.

WHAT WOULD MY PARTICIPATION INVOLVE?

If you decide to participate, you will take part in an interview that will take approximately 30 minutes. In this interview, questions will be asked on various topics related to privacy and data security.

Your participation in this research is entirely voluntary, and you can withdraw at any time. You are free not to answer any questions. We believe there are no known risks associated with this research. Your responses in this research will be kept confidential to the best of our ability. We will minimize any risks by securely storing the data on UT servers and removing unnecessary personal data.

However, it is not possible to remove your data from the project after it has been anonymized because we will no longer be able to identify your specific data. This does not affect your data protection rights. If you decide not to participate, you do not need to take any further action.

DATA PROTECTION AND CONFIDENTIALITY

To participate in this research project, we need to collect information that could identify you, known as “personally identifiable information”. Specifically, we need the following data:

- Your gender
- Your age
- Educational level
- Employment status
- Duration of employment

All data collected during the interview is only available to the researcher (Jesper Walinga) and the supervisors (Ton Spil and Maarten Renkema) involved in this project. The data will only be used for academic purposes. It contributes to the writing of my master thesis and other research publications that may arise from it. Any publications resulting from this research will not identify you as a source of information. A copy of the research results is available to you if you wish.

CONTACT DETAILS

If you have questions about the research or if you are interested in participating, please contact the researcher:

JESPER WALINGA, e-mail: j.p.walinga@student.utwente.nl

Or the supervisor:

TON SPIL, e-mail: a.a.m.spil@utwente.nl

Consent form for interview – Master Thesis

YOU WILL RECEIVE A COPY OF THIS SIGNED CONSENT FORM

Tick the right boxes	Yes	No
Participation in the research		
I have read and understood the study information dated [dd/mm/yyyy] or it has been read to me. I have had the opportunity to ask questions about the research, and my questions have been answered satisfactorily.	○	○
I voluntarily agree to participate in this research and understand that I can refuse to answer questions and that I can withdraw from the research at any time without giving a reason.	○	○
I understand that participating in the research involves being interviewed.	○	○
Use of information in the research		
I understand that the information I provide will be used for writing a master thesis and other research publications that may result from it.	○	○
I understand that personal information collected about me that can identify me (e.g., my name or where I live) will not be shared outside the research team.	○	○
I agree that my information can be cited in research results.	○	○

Signature
Name:
Signature:

Study contact details for more information:
Jesper Walinga, j.p.walinga@student.utwente.nl or Ton Spil, a.a.m.spil@utwente.nl

Contact details for questions about your rights as a research participant:
If you have questions about your rights as a research participant, would like to obtain information, ask questions, or discuss concerns about this research with someone other than the researcher(s), please contact the secretary of the Ethics Committee of the Faculty of Behavioural, Management and Social Sciences at the University of Twente. You can reach them via the following email address: ethicscommittee-hss@utwente.nl

Appendix 3. Information form

Information form for participation in Medical-Scientific research

Dear Sir/Madam,

We are asking if you would like to participate in a scientific research study. Participation is entirely voluntary; you decide whether you want to participate. Please read the information carefully, and if you have any questions, you can contact the researcher. By participating in this research, you contribute to science and the development of WOPiT. This letter contains information about this research.

What is the aim of the research?

The aim of this research is to map out the views and knowledge of employees on privacy and data security-related topics. Afterwards, WOPiT will receive advice or a tool that improves or maintains awareness of these topics. Your input is therefore incredibly important to provide the most appropriate follow-up to this research.

What does you participation involve?

If you decide to participate, the researcher will conduct an interview with you. The interview will last approximately 30 minutes. During this interview, questions will be asked about privacy and data security-related topics. The audio of the interview will be recorded. Your name will be known to the researcher at the time of the interview but will not be part of the data collection. During the recording, your name will not be mentioned so that the interview cannot be traced back to you. Also, in reports and any publications of this research, the results of the interview cannot be traced back to you. If you have any questions or complaints about this, we ask you to contact the researcher.

If you do not want to participate or wish to stop the research

You decide whether you participate in the interview. If you participate, you can always change your mind and stop, even during the interview. You do not need to provide reasons for ending the interview. The answers collected up to that point will be used for the research without your objection. If you object, the collected data will be destroyed

Thanks for your attention.

Researcher: Jesper Walinga, j.p.walinga@student.utwente.nl
Supervisor: Ton Spil, a.a.m.spil@utwente.nl

Appendix 4. Interview scheme

General information
Respondent number:
Date:
Start time:
End time:

Introduction

Good morning/afternoon, my name is Jesper Walinga, and I am studying for a master's degree in Health Sciences at the University of Twente in Enschede. I am currently working on my graduation research, and this interview is part of it. The research is about the views and knowledge of employees regarding privacy and data security-related topics within WOPiT.

The purpose of this interview is to map out the views and knowledge of employees on privacy and data security-related topics. Afterwards, WOPiT will receive advice or a tool that improves or maintains awareness of the topics. Your input is therefore incredibly important to provide the most appropriate follow-up to this research.

The information collected from this interview is confidential and processed anonymously. This means that no information can be traced back to you in the final report. Before we begin, I would like to ask your permission to record this interview. I will use the recording to listen back for my analysis. Do you agree to the recording? I will also ask this after the recording has started so that it is included in the recording. I hereby hand you the consent form.

Sign consent form

In this interview, I will ask various questions where there are no right or wrong answers. At any time, you have the option to stop the interview or not answer a specific question. If you do not understand a question, please ask for clarification. During the interview, I may take notes. The interview will last approximately 30 minutes.

Do you mind if I address you informally?
Do you have any further questions before we start the interview?

I will now start the recording.

start recording

Do you agree to the recording of this interview?

Personal information
First, I would like to ask you for some personal information.

- What is your age?
- What is your gender?
- What is your educational level?
- What is you employment status and duration?

Topics
I will ask questions about different themes which are important for this research about privacy and information security at WOPiT.

Security (informatie security)

- Based on your working experience, tell me about your security-related concerns, if any, within your daily work at WOPiT?
    - Where do these concerns come from?
    - What is done with your concerns?

- What security measures do you encounter in your daily work?
    - Think of passwords, access to information only by members of you own location, etc.
    - What do you think of all these measures?

- What constitutes a data breach?
    - How do you handle a data breach? Or if you find out there is a data breach?
    - Why do you handle it this way?
    - What is WOPiT's policy on a data breach?
    - Does the policy influence your actions? And in what way?
    - How do you think such situations are handled?
    - n data lek? Of als u er achter komt dat er een data lek is

Privacy

- Based on your working experience, tell me about your privacy-related concerns, if any, within your daily work at WOPiT?
    - Where do these concerns come from?
    - What is done with your concerns?

- What privacy measures do you encounter in your daily work?
    - Think of whether or not to use names, e.g. incident reports.
    - What do you think of all those measures?

Policy

- What steps do you take if you have a question or encounter a situation where you do not know WOPiT's policy?
    - Why these steps? (instinct, trained, policy)

- To what extent are you aware of WOPiT's policy?
    - Do you know where to find it?
    - Do you know what it says?

- How much attention is given to vigilant working during the training period?
    - What do you think of that amount of attention to this topic?
    - Are these recurring topics even after the training period? In other words, is knowledge/awareness maintained?
        - If yes, in what form?
        - If no, what do you think of this?

Ethics

Throughout you career, you have to make various ethical considerations, and you may sometimes have to break agreed rules. Sometimes you weigh whether you MUST share information in the interest of WOPiT, member in question, or other members. (Provide an example if necessary)

- How do you handle issues like the ones described above?
    - What considerations do you make?
    - With whom do you make the final decision, and do you share your thinking?
    - How do you prioritize?

Trust

I am now going to ask some questions about trust. Both trust in your own ability and trust from and towards others. You may answer the question in the context of privacy, etc.

- Do you trust that you do your job well? (minimize mistakes)
    - Where does that trust come from? (Aware of rules, well-trained, never heard it was not good)

- To what extent do you feel the trust of your colleagues that you do your job well?
    - What shows this?

- To what extent do you trust your colleagues to do their job well?
    - If you have doubts, what steps would you take?

- To what extent do you trust that the rules ultimately benefit the care and the care system?
    - Where does that come from?

Confidentiality

As you know, the information you collect about members during your work is confidential. You should not share information without permission.

- Based on your working experience, tell me about your confidentiality-related concerns, if any, within your daily work at WOPiT?
    - Where do these concerns come from?
    - What do you do with your concerns?
    - What is done with your concerns?

Safety (member safety)

- To what extent do you consider the safety of members when you record in the file?
    - Think about wording things less severely than they might be.
    - Would you write thing differently if the member did not have access?
        - Why?

- To what extent do you consider your own safety when you record in the file?
    - Think about wording things less severely than they might be.
    - Would you write thing differently if the member did not have access?
        - Why?

Conclusion

I have reached the end of the interview. Is there anything that has not been covered that you would like to mention? Do you have any questions for me?

Thank you for your participation. I will now stop the recording. If you have any questions or comments later, you can reach us at the contact details provided in the information letter for this research.

Appendix 5. Overview themes with corresponding codes

Themes and corresponding codes	Fragments (n=213)	Participants (N=7)
Security	44	7
Technical safeguard	19	7
Physical safeguard	12	7
Concerns	7	6
Opinion	6	6
Privacy	39	7
Pseudonymization	16	7
Awareness	13	7
Opinion	5	5
Concerns	4	4
Consent form	1	1
Trust	35	7
Colleague trust	14	7
Competency	14	7
System trust	7	7
Policy	32	7
Handling	11	7
Training period	10	7
Knowledge	6	6
Recurring theme	5	5
Data breach	30	7
Handling	15	7
Meaning	8	7
Policy	6	6
Opinion	1	1
Confidentiality	11	6
Honesty	6	5
Sharing at home	5	5
Ethics	11	6
Handling	11	6
Safety	11	6
Member access	11	6