Journal of the Association for Information Systems (2022) **23**(1), 237-263
doi: 10.17705/1jais.00717

RESEARCH ARTICLE

ISSN 1536-9323

The Design of a System for Online Psychosocial Care: Balancing Privacy and Accountability in Sensitive Online Healthcare Environments

Jonas Sjöström[1], Pär Ågerfalk[2], Alan R. Hevner[3]

[1]Department of Informatics and Media, Uppsala University, Sweden, jonas.sjostrom@im.uu.se
[2]Department of Informatics and Media, Uppsala University, Sweden, par.agerfalk@im.uu.se
[3] Muma College of Business, University of South Florida, USA, ahevner@usf.edu

Abstract

The design of sensitive online healthcare systems must balance the requirements of privacy and accountability for the good of individuals, organizations, and society. Via a design science research approach, we build and evaluate a sophisticated software system for the online provision of psychosocial healthcare to distributed and vulnerable populations. Multidisciplinary research capabilities are embedded within the system to investigate the effectiveness of online treatment protocols. Throughout the development cycles of the system, we build an emergent design theory of scrutiny that applies a multi-layer protocol to support governance of privacy and accountability in sensitive online applications. The design goal is to balance stakeholder privacy protections with the need to provide for accountable interventions in critical and well-defined care situations. The research implications for the development and governance of online applications in numerous privacy-sensitive application areas are explored.

Keywords: Privacy, Accountability, Psychological Healthcare, Scrutiny, Design Science Research, Design Theory

Sudha Ram was the accepting senior editor. This research article was submitted on January 4, 2019 and underwent three revisions.

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation." Universal Declaration of Human Rights by the United Nations (1948)

1 U-CARE: An Online System for Psychological Care

Our research context is the large-scale, multidisciplinary research program Uppsala University Psychosocial Care Programme (U-CARE). The program is funded primarily by grants from the Swedish Research Council. The multidisciplinary program involves researchers and practitioners from the fields of psychology, medicine, information systems, the caring sciences, and economics. The foundation of the project is the implementation of a sophisticated software system for online psychosocial care with comprehensive support for online clinical trials. Stakeholder (e.g., patient, caregiver) privacy concerns make the development and use of the U-CARE system challenging with highly sensitive privacy and accountability requirements.

As discussed in Grönqvist et al. (2017), U-CARE aims to establish a high-impact research environment (c.f., Nunamaker et al., 2017) in the area of online psychosocial support to distributed and vulnerable populations with potentially lethal somatic diseases. The goal is to contribute to knowledge on coping with post-traumatic stress caused by their diagnosis, which may lead to depression and anxiety and possibly impair recovery from the somatic disease. For example, a depressive state may cause a patient to engage in less physical activity, to develop sleeping problems, or to forget to adhere to their medications. Internet-based self-help has proven effective for psychiatric disorders as well as for the promotion of healthy behaviors (Barak et al., 2008; Riley & Veale, 1999). An online caregiving environment has shown promise, impacting both treatment efficacy and cost, by using less therapist time per effectively treated patient compared to face-to-face therapy (Tate & Finkelstein, 2009).

The online support environment employs a stepped-care strategy that directs patients with mild depression or anxiety to a self-help program. In contrast, patients with more severe depression or anxiety are offered a treatment program based on cognitive behavioral therapy (CBT) (Riley & Veale, 1999). Also, patients become part of an online community, allowing them to interact with peers and health staff in discussion forums, online chats, and internal peer-to-peer messages.

In this paper, we report on the longitudinal U-CARE design science research (DSR) project in the eHealth domain and its significant impacts on both research and practice. We present the project as a series of development cycles with concise descriptions of designed artifacts and their evaluation in each cycle. Throughout the development cycles, we build an emergent *design theory of scrutiny* (ToS) for sensitive online systems. The theory concerns online interactive environments that provide privacy guarantees while accountability is maintained and easily inspected. We show how the ToS evolves through the design of a multilayer protocol for supporting privacy and accountability in online applications. We present a formalized conceptual model of a supportive environment that maintains anonymity yet preserves well-defined metalevels of governance and control. The contributions of the U-CARE project are evidenced by their impacts on both practice and research realized through the development of an innovative software and support environment for the provision and study of online psychosocial support. That is, we provide both technological and theoretical contributions (Baskerville et al., 2018; Ågerfalk and Karlsson, 2020). In doing so, we directly address the DSR "gulf [that] exists between theoretical propositions and concrete issues faced in practice" (Lukyanenko & Parsons, 2020, p. 1343). Our combination of technological and theoretical contributions represents what Iivari (2020) refers to as new design knowledge, which includes knowledge about both the design product and the design process. That is, we report knowledge about a novel IT artifact with practical utility.

We structure the paper accordingly by providing a faithful account of how the artifacts and theoretical insights emerged in tandem. We begin with a survey of the multidisciplinary research background of the privacy and accountability of computer information systems. Section 3 presents the DSR research methods and our design theory development approach (further explained in Appendix A). Section 4 describes the first development cycle for the U-CARE software system, which led to reflection and the initial proposal of our design theory of scrutiny. Section 5 lays out the theory of scrutiny in greater detail and proposes a set of design principles for the provision and governance of privacy and accountability. Section 6 explores the second development cycle of the U-CARE software system as used and evaluated in a real-world set of clinical trials. Finally, we discuss the results and explore the wide-ranging theoretical and practical implications of the research project.

2 Privacy and Accountability in Information Systems

The rise of online communities and social media as a vehicle for large-scale social interactions has accelerated the penetration of information technology (IT), information systems (IS), and application platforms (Parker et al., 2016) into both private and professional life (Aakhus et al., 2014). A significant part of contemporary social interaction is planned and mediated on digital IT platforms (Nambisan et al., 2017). Although this evolution of human collaboration and social life may be beneficial in many ways, it also portends a significant threat to individual privacy (Bélanger & Crossler, 2011). Two forces fuel the threat to privacy. The first force is the growth of IT, which, in itself, enables increased functional capabilities, storage capacities, networking connections, and surveillance reach. The second force is that commercial actors find value in information about individuals, causing them to seek ways to exploit technological opportunities to collect and capitalize on such information (Mitnick & Vamosi, 2017). Notably, one's right to privacy, i.e., freedom from unauthorized intrusion and arbitrary interference with privacy, is a human right as declared by the United Nations (1948).

2.1 Basic Constructs

Three central constructs for this research are scrutiny, privacy, and accountability. We define information systems "scrutiny" as a process, with the ultimate goal of protecting privacy while ensuring responsible, accountable use of an information systems artifact. Scrutiny consists of recurring activities and protocols to identify and mitigate the misuse of personal information in an accountable manner.

Albeit deceptively straightforward, it is not easy to define the term "privacy." A value-based definition views "general privacy as a human right integral to society's moral value system" (Smith et al., 2011, pp. 992-993). While such a definition is highly normative, researchers in information systems and other social sciences frequently adopt other views, such as privacy being "the ability of individuals to control the terms under which their personal information is acquired and used" (Culnan, 2003 p. 326). In this work, we subscribe to the normative definition, while still acknowledging that the ability of individuals to maintain control of their information is an essential consideration in IS design (Kordzadeh & Warren, 2017). Bélanger and Crossler (2011) provide a comprehensive survey and meta-analysis of IS research on privacy.

According to ethnomethodologist Harold Garfinkel (1967, p. vii), actions that are "accountable" are "visibly rational and reportable for all practical purposes," a notion that is at the heart of information accountability. We align our thinking with Weber's (1978) classical definition of social action as "that human behavior to which the actor attaches meaning and which takes into account the behavior of others and thus is directed in its course." Garfinkel's view suggests that an accountable IS must keep a record of the social actions performed through and by the system (both their social grounds and their social purposes) as a sociopragmatic instrument for communication (Goldkuhl & Ågerfalk, 2005; Ågerfalk, 2020).

Weitzner et al. (2008, p. 84) approach accountability from an online web infrastructure perspective, stating that "information should be transparent so it is possible to determine whether a particular use is appropriate under a given set of rules and that the system enables individuals and institutions to be held accountable for misuse." They propose three architectural features to facilitate transparency and information accountability:

1. Policy-aware transaction logs that record "information-use events" are required. Each endpoint in a decentralized system should keep such logs. The point of the logs is that they facilitate follow-up on information use and misuse.
2. A common framework to represent policy rules is needed. Semantic web technology would be the foundation for such frameworks, which would emerge through the collaboration of large overlapping communities on the web.
3. Policy-reasoning tools to support users in understanding how they may use the data they knowingly or unknowingly share. Such information would be made possible through the visible policy rule frameworks and compelling user interfaces that raise users' accountability perceptions (Vance et al., 2015).

Weitzner et al.'s architectural features are suggestions to improve the infrastructure of the Web to promote accountability on a grand scale. Inspired by these features, our design process emphasizes (1) recording information use, (2) clarifying policy rules, and (3) supporting users in understanding the legitimate use of data. We expand on the design implications below when detailing the action-oriented architecture (Section 4.3) and its use (Section 6).

2.2 Anonymous Behaviors and Accountability

A critical approach to facilitating privacy is providing anonymity. Anonymous interaction between peers is at the heart of the design of online communities. The so-called disinhibition effect (Suler, 2004) suggests that people say and do things online that they would not say or do face to face. On the one hand, people may beneficially contribute to discussions in an online forum that they would not have, had the discussion occurred offline. On the other hand, anonymity creates the risk of undesired behaviors that may negatively affect the online community, such as bullying or the provision of links to illegal activities (e.g., sex and drugs). There are well-known examples of the consequences of unethical online behavior from discussion forums, blogs, and online newspapers, such as the closedown of user comments on the Engadget forum (Zhuo, 2010).

In an attempt to tame the negative consequences of the disinhibition effect, online publishers are increasingly referring comments to other forums, such as Facebook, that do not enforce anonymity to the same extent (Thorén et al., 2014). However, recent revelations about the disclosure of user data to Facebook's business partners (e.g., Cambridge Analytica) have led to widespread distrust of the adequacy of privacy safeguards on Facebook (Dance et al., 2018). Social networking platforms, such as Twitter and Facebook, are facing many individual lawsuits and governmental investigations regarding their privacy and accountability policies.

It is imperative for a trusted social network provider, particularly in the healthcare sector, to proactively monitor community behaviors, identify detrimental behaviors, and take appropriate actions when such behaviors occur. From the community provider perspective, such actions concern accountability, i.e., how to hold people accountable when their behaviors deviate from the norms of the community (Vance et al., 2013; Vance et al., 2015). The beginning of comprehensive system accountability relies on transparency in the design and use of the information technologies and software system platforms that underlie the social network environment (Weizner et al., 2008; Sjöström, 2010). Increased transparency implies a need for extensive logging of what people do in the social network system. However, the very mechanism to mitigate information misuse, logging, poses an additional risk for misuse. The tension between privacy and accountability creates a challenge for designers to preserve privacy while at the same time ensuring accountability.

We observe from our survey of the research literature that privacy and accountability have traditionally been addressed primarily from a technical security perspective, and there is a lack of research that provides a holistic systems view of the individual, the organization, and society. Belanger and Crossler (2011) call for more design science research on privacy in their meta-analysis of privacy research in the IS domain. Thus, the U-CARE context provides a unique research opportunity to report in detail on the design and implementation of sophisticated software for a sensitive online healthcare environment with requirements for privacy and accountability. In the following, we describe the innovative design of the U-CARE software and the development of a design theory of scrutiny, thus answering the call in Baskerville et al. (2018) for finding a balance between artifact and theory in DSR.

3 The U-CARE Research Project

A fundamental premise of design science research (DSR) in the field of information systems is to allow for the publication of novel IT artifacts as bona fide research contributions (Hevner et al., 2004; Ågerfalk, 2014; Ågerfalk & Karlsson, 2020). U-CARE is an ongoing multidisciplinary research program, including DSR-based information systems research (Hevner, 2007; Gregor & Hevner, 2013). The system was initially developed in two development cycles, as shown in Figure 1. First, a discovery and demonstration cycle (2011 to mid-2012) built the initial software while, in parallel, formulating the theory of scrutiny (ToS) based on relevant kernel theory and extensive domain knowledge (Sjöström et al., 2014). Following this cycle, we conducted a second cycle of implementation and evaluation (mid-2012 to mid-2016). At this point, the system was adopted by the U-CARE practice, continuously refined, and populated with live data. Evaluations during this cycle involved actual use of the software for 11 clinical trials of psychosocial support for patient populations. This cycle extended and evaluated the ToS based on the support of user privacy and accountability in the implemented system, as described in Section 6.

A basic premise for our theorizing process is that design and intervention in a particular domain serve to develop knowledge about the domain (Baskerville & Myers, 2004; Baskerville et al., 2015). The setup of an eHealth practice, including the design of supporting software (in our case, the Cycle 1 version of the U-CARE system), provided us with experience from both the *process* of design and the software system design as an *artifact*. Theorizing consisted of reflecting and learning from those experiences, i.e., generalizations from empirical data to theory (Lee & Baskerville, 2003). Through a series of iterations, practice and technology emerged. In keeping with pragmatism, we conceive of design theory as a practical means to aid inquiry (Dewey, 1938) that encompasses both design and evaluation and seeks to change a problematic situation into a preferred one. Thus, our theory development did not aim for deductively validated hypotheses but for theoretically and empirically justified propositions. Hassan et al. (2019, p. 200) express the need for a stronger focus on the context of discovery in IS research: "The creativity of the researcher is most strongly pronounced within the context of discovery and foregrounding this stage of theorizing allows us to understand the researchers' creative strategies that led them to realize their goals." Consequently, we attempt to balance the contexts of discovery and justification in this paper. In Section 6, we provide a more thorough discussion of our approach for grounding the development of the U-CARE platform and the design theory of scrutiny. Appendix A provides a further explanation of our approach to theorizing in DSR. Previous reports from U-CARE (Sjöström et al., 2014; Grönqvist et al., 2017; Mustafa, 2019) provide in-depth discussions about the complexity of multidisciplinary research in eHealth, further demonstrating the wickedness of the design context.

We note that Cycle 1 and Cycle 2 are not distinct periods; they instead signal that the organization and its technology concerning scrutiny issues made a transition to "implementation and use mode" rather than "design and construction mode." They also signify a transition in focus from *discovery* (the process of abductive inferences that devises plausible and promising propositions) to *justification* (the process that evaluates those propositions by studying the artifact in use). After two years of system use, we revisited the practice to investigate the actual use of the software (the populated system) and the establishment of management routines (governance) related to scrutiny. Essentially, this facilitated an assessment of the ToS and related kernel theories adopted initially to inform the design and supported deep reflection about their qualities as a foundation for generalizing theories of scrutiny governance in organizations.

4 Designing the U-CARE System (Cycle 1)

We present a summary of the activities performed during Cycle 1 of the development of the U-CARE software system. Considerable efforts by the development team were devoted to understanding the psychosocial care environment and issues of privacy and accountability. Comprehensive requirements were generated for the development of the initial prototype of the U-CARE system.

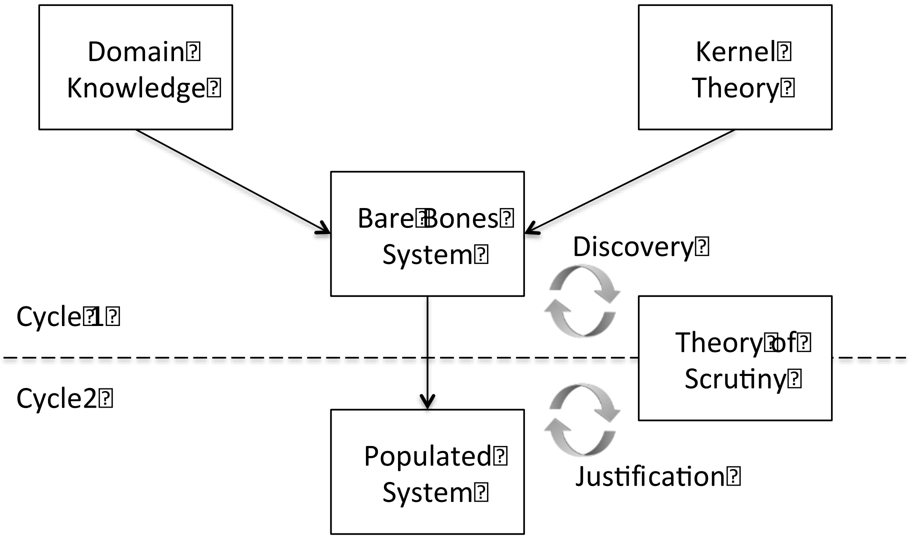

Figure 1. Schematic Representation of the Applied DSR-Based Theory Development Approach

4.1 Demonstration System

The development approach followed Scrum agile methods (Scrum Alliance, 2018), including biweekly sprint meetings with various stakeholders from the U-CARE context. These meetings included researchers, medical doctors, nurses, patient groups, and psychologists, who provided feedback on the emerging software design. We conceived of this process as formative evaluations of the emerging software; in total, we held 100+ workshops between 2011 and 2015. Most system features address requirements from psychologists and researchers. Psychologists contributed ideas on how to deliver stepped care online, including self-help, cognitive behavior therapy, and peer interaction in forums and chat. Researchers contributed with ideas on how to support randomized controlled trials (RCTs) online, i.e., designing questionnaires, launching them according to study-specific rules, and sending SMS and email reminders to patients and stakeholders to improve adherence to the study. Also, various features to monitor progress in studies and enable therapist decision-making (Sjöström & Alfonsson, 2012) were built into the system to support interactions among psychologists, researchers, and developers.

4.2 An Action-Oriented Architecture for Accountability

Designing for accountability and scrutiny requires a system architecture that can capture relevant information about the social interaction performed throughout the system. Traditional approaches to data management pay little attention to the social and pragmatic aspects of information and its use in social practices (Aakhus et al. 2014). The use of Scrum did not necessarily help us address such issues either. It may have helped us identify stakeholder requirements related to privacy and accountability, i.e., promoting relevance, but it did not guide the design and implementation of such requirements. Therefore, in order to construct a solid foundation for accountability, we draw on the pragmatic and action-oriented approach to conceptual modeling (AOCM) described by Ågerfalk and Eriksson (2004) as a kernel theory to support design. This approach distinguishes itself in two regards: First, it acknowledges the speech-act theoretical insight (Searle, 1969) that languages, and thus information systems, are used for other purposes than just describing a real world outside the system. Second, it emphasizes what speaking does, in addition to what is spoken about.

The AOCM approach stresses that actions in and by themselves constitute essential objects for which we need to store information. For instance, instead of viewing a business process only in terms of an order that changes state from offer to order and then to invoice, these three concepts represent critical business actions and need to be treated as separate entities in conceptual models and resulting database schema. Thus, the interplay between static and dynamic conceptual modeling becomes critical. In AOCM, dynamic models are not merely a means to show how entities of a static model change over time but essential sources of knowledge for creating the static model (e.g., identifying social actions that should constitute objects).

In the U-CARE context, the adoption of AOCM facilitated the required retrospective analysis of what commitments were made and acted upon by the various actors using the software. Within the frame of AOCM, the architecture employs the model-view-controller (MVC) pattern and role-based access control (RBAC) (Wainer et al., 2007).

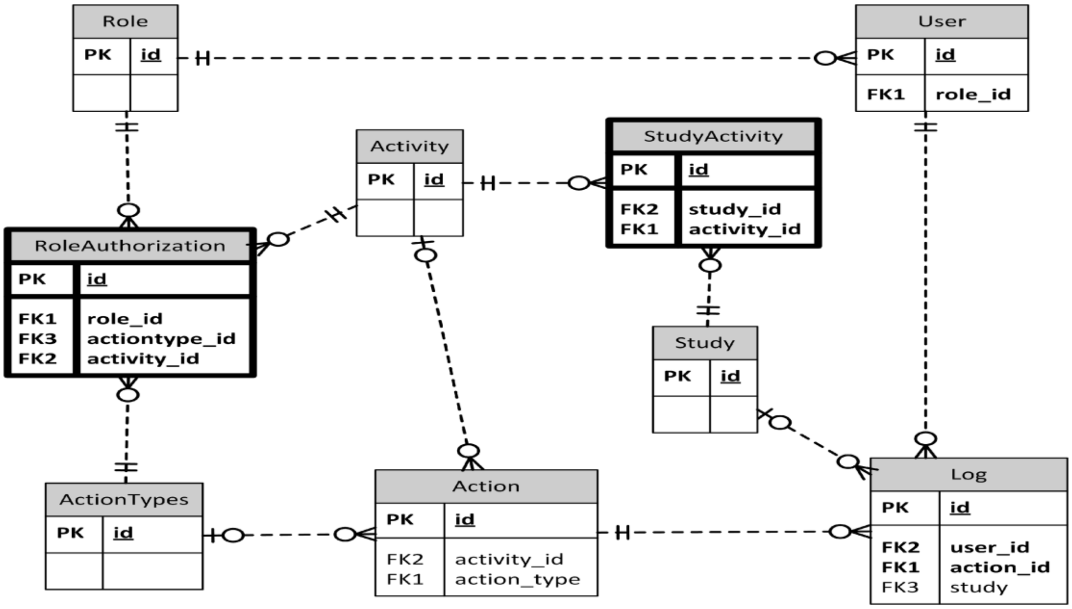

Figure 2. Static Design of the U-CARE Action Framework

Figure 2 illustrates the "action framework" as implemented in the U-CARE software drawing from AOCM concepts. The figure—a subset of the U-CARE database model—facilitates the tracking of users, their roles, and actions performed in the business context. For instance, it informs us how the user "Pietrov," whose role is "therapist," performed the action "respond to submitted homework assignment" at a specific time. The context of the action is the action type "provide" in the activity "cognitive behavioral therapy." The design thus allows us to query social interactions taking place through the software and to filter those queries based on a conceptualization of actions based on terminology relevant to the domain (in this case, to psychosocial care).

Further, authentication and authorization to perform actions are managed through the authorization of roles that are to perform certain action types in certain activities. A therapist, for instance, would be allowed to "provide" (i.e., a type of action) in the "cognitive behavioral therapy" activity through a role authorization. Activities can also be switched on and off, allowing for flexible use of features, such as chat and forum, tailored to the needs of each particular study.

A dynamic filter implemented in the system manages authorization and logging. A client making a request to the webserver invokes the filter code, as diagrammed in Figure 3. The filter assures (1) proper authentication of the user and the requested action, and (2) logging of the action. Sjöström et al., (2017) outline a technological perspective on the action framework, including metarequirements for design.

In summary, the Cycle 1 U-CARE design promotes accountability by being ingrained with three kernel theories: AOCM, RBAC, and MVC, resulting in a novel authorization scheme; governing access to perform accountable social actions using the software based on the actor role. The database design (Figure 2) supports managing business action metadata in the database inspired by AOCM. This metadata connects each user's right to perform actions (RBAC) to specific software functions (i.e., MVC controller actions), thus tying the three kernel theories together. The dynamic design (Figure 3) shows the corresponding logical flow of authorization and logging actions. This novel combination of kernel theories made the architecture and proposed design for accountability possible. Although industrial uptake of AOCM is so far limited, it provides a theoretically grounded yet practical approach to going beyond the received view of representation theory in IS. Several calls for such pragmatic grounding of conceptual modeling have recently been made (March & Allen, 2014; Aakhus et al., 2014; Burton-Jones et al., 2017; Eriksson et al., 2018), and the U-CARE design provides a much-needed proof of concept. In the static model, we have thus exapted knowledge from various sources to design a novel and generalizable solution for privacy and accountability.

4.3 Initial System Evaluation

The evaluation of the U-CARE software in Cycle 1 consisted of the successful implementation of an expository instantiation (Gregor & Jones, 2007) as a proof of concept. We fine-tuned the system over time to improve performance and correct bugs, but the conceptual design (partially shown in Figure 2 and Figure 3) remained constant during Cycle 1. The action framework, as initially designed, produces log data that support full transparency of all social interaction.

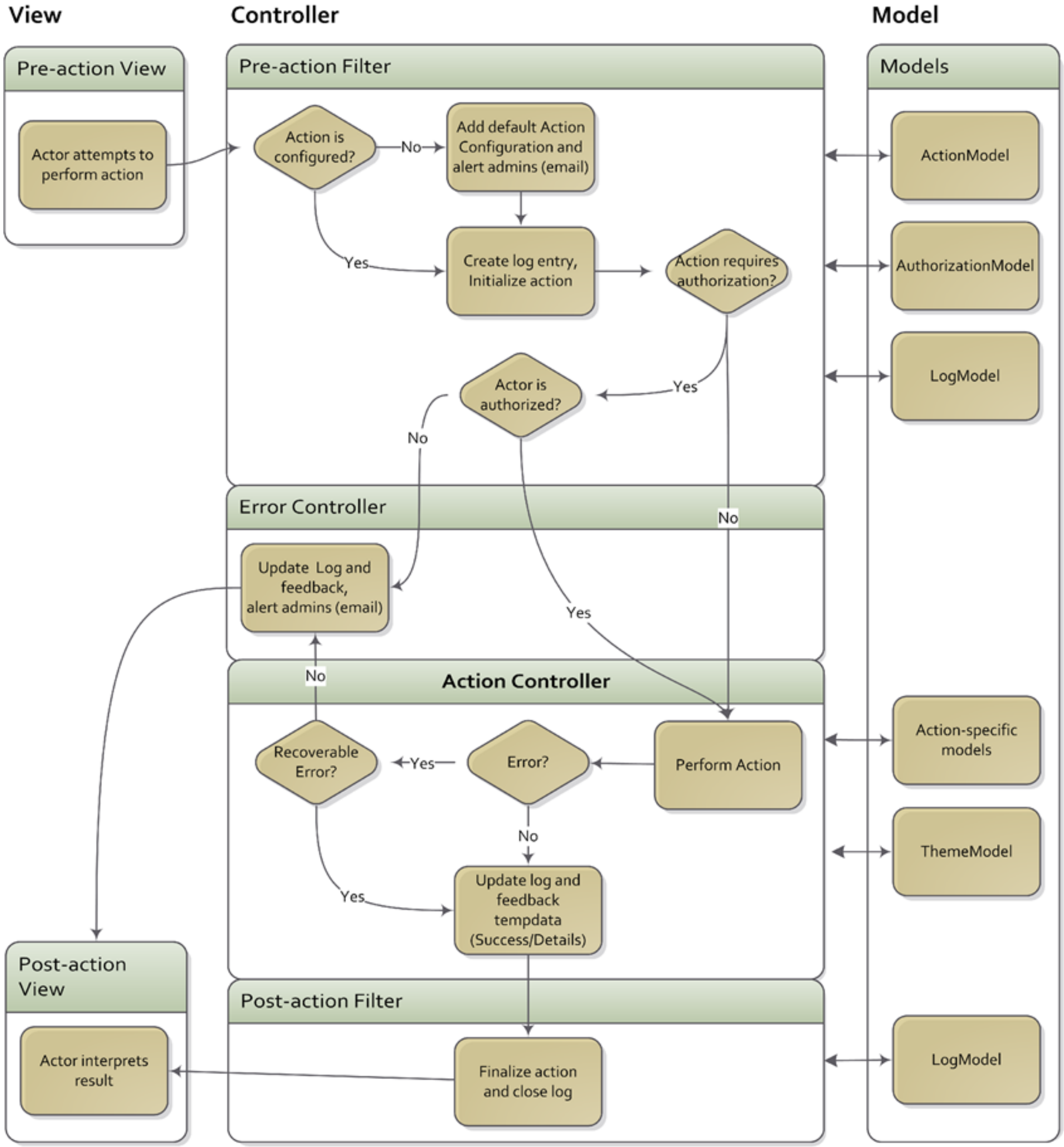

Figure 3. Dynamic Design of the U-CARE Action Framework

By the end of Cycle 1, there were metadata for ~500 organizational actions and ~20 activities in the database. The system prototype demonstrates clearly that the proposed solution to pragmatic logging was feasible to implement and that it permitted comprehensive conceptualization and logging of business actions conducted by authenticated users. We elaborate further on the evaluation of the proof of concept in our Cycle 2 evaluation in Section 6.1.

5 A Design Theory of Scrutiny

During the first cycle of system design, implementation, and evaluation, we began the research process of generalizing our findings to a design theory of scrutiny (ToS) that could be applied to a broader range of IS applications. The development of this design theory is grounded in our experiences with the U-CARE system design and the existing knowledge base of design theory in the field of DSR (see Appendix A for a concise review of this design theory knowledge base). Sjöström et al. (2014, 2017) present earlier versions of ToS. ToS, as presented here, is elaborated and substantially more theoretically justified and evaluated. Furthermore, we present the full story of ToS, including the research process and thorough examples that convey the design rationale for the U-CARE software.

ToS consists of different elements serving as an instrument to support inquiry into scrutiny practices and software design. In Section 5.2, we express our codified understanding of how best to balance privacy and accountability as a multilayered protocol based on the modes of scrutiny as defined in Section 5.1. The multilayered protocol, drawing from the U-CARE design experience and inspired by Belanger and Crossler's (2011) call for research addressing the relationship between societal, organizational, and individual privacy issues, is used as a premise to conceptualize scrutiny control flows (Section 5.3) concerning privacy expectations and accountability information. Sections 5.1-5.3 are instruments for inquiry, supporting structured discussions and focused reflections on the management of privacy in organizations (see Appendix A for a more elaborate discussion on inquiry and practical theory). Section 5.4 is a design-oriented operationalization of the multilayered protocol into scrutiny design principles.

5.1 Levels of Scrutiny

In the design process, we inductively identified four groups of eHealth stakeholders regarding scrutiny (Table 1): societal institutions (e.g., government agencies and the media), principals (e.g., community providers), agents (e.g., the staff operating on behalf of principals), and peers (e.g., community members).

Scrutiny is an activity that involves various stakeholders who engage in different modes of activity concerning privacy and accountability. The conceptual difference between these modes provides a structure to analyze an online system regarding its capabilities to maintain organizational responsibilities and accountability while protecting individual privacy. A fundamental proposition is that violation of privacy should be either (1) well-motivated, based on organizational responsibility, or (2) accounted for by someone. We briefly review each of the scrutiny levels from external to internal.

Level 3 scrutiny explains the processes in society that shape and force stakeholders to comply with ethics and legislative regulations regarding privacy and accountability. This level includes traditional external auditing practices but extends beyond what is legally required in order to also encompass tacit expectations that external stakeholders may impose on an organization.

In order for the organization to be ready to respond to such external scrutiny, there is a need for ongoing Level 2 scrutiny. Such scrutiny requires the organization to stay updated about the external requirements and to set up internal processes to log and monitor the use (and misuse) of sensitive information about individuals. This level is thus comparable to the traditional IT controller function in an organization but goes beyond budgetary control to include employee behavior in the broader sense. In order to adequately manage such controls, the organization needs to monitor legislative changes and externally imposed requirements for privacy and accountability.

Level 1 scrutiny occurs when staff members responsibly monitor community activity following organizational policies and external requirements. Potential misuse may stem from less responsible staff behavior resulting in information misuse that should be "detected" in Level 2 scrutiny.

Privacy concerns are also subject to Level 0 scrutiny, which refers to the community members' peer controls for monitoring system interactions. For example, community members should have the ability to personalize their visibility, to block others' activities, and report unauthorized content. Level 0 scrutiny also entails activities in which community members take some responsibility for the societal discourse, the community providers' privacy policies, and staff behaviors.

5.2 Scrutiny Protocol Matrix

Given the above-identified stakeholders, we propose the *scrutiny protocol matrix* in Table 2, which shows the possible combinations of scrutinizers and scrutinized. The columns in the matrix show four different types of accountability: societal accountability, principal accountability, agent accountability, and peer accountability. The rows in the matrix correspond to the different levels of scrutiny outlined in Table 1, denoted as Level 0 – Level 3. The conceptual differentiation between the level of scrutiny and type of accountability provides a sophisticated structure to analyze an organization concerning its capabilities to maintain organizational responsibilities and accountability in relation to relevant stakeholders.

Societal accountability refers to the scrutinization of societal institutions. It concerns society's self-sanitizing processes in terms of public discourse and policy development related to privacy (Level 3), as well as community provider management's (Level 2), staff members' (Level 1), and community members' (Level 0) monitoring of laws and ethics that concern privacy. What is at stake here is the societal responsibility regarding individuals and organizations.

Principal accountability refers to the scrutinization of community providers. At Level 3, it concerns societal institutions' scrutiny of community providers' compliance with applicable privacy laws and ethics. At Level 2, it refers to community providers' self-scrutiny, such as assessing whether internal processes and policies fulfill stated and unstated privacy requirements. At subsequent levels, it refers to staff members' (Level 1) and community members' (Level 0) scrutiny of corporate routines related to privacy and accountability. What is at stake here are the responsibilities of community providers, as principals, regarding societal and individual interests.

Table 1. Four Levels of Scrutiny

Mode	Scrutinizer	Accountable	Activity
Level 0 Scrutiny	Community member(s)	Community member(s)	At the peer-to-peer user level, identify and mitigate community behavior that does not conform to the organizational norms and individual privacy preferences.
Level 1 Scrutiny	Staff member(s)	Community member(s)	At the staff-to-user level, identify and mitigate community behavior that does not conform to the organizational norms.
Level 2 Scrutiny	Provider Management	Staff member(s)	Log and monitor actions to protect privacy concerns and uphold accountability.
Level 3 Scrutiny	External stakeholders	Provider Management	Audit organizations to validate compliance with legislation and ethics.

Table 2. The Scrutiny Protocol Matrix

		Societal accountability	**Principal accountability**	**Agent accountability**	**Peer accountability**
	Scrutinized / Scrutinizer	**Societal institutions**	**Community provider**	**Staff members**	**Community members**
Level 3 scrutiny	Societal institutions	Public discourse on privacy and accountability	External scrutiny of community providers' compliance with privacy laws and ethics	External scrutiny of staff members' behavior	External audit/scrutiny based on direct access to community interaction data
Level 2 scrutiny	Community provider	Management monitors laws and ethics concerning privacy concerns	Management performs self-scrutiny, i.e., assessing whether their processes and policies sufficiently fulfill privacy ideals	Management ensures that staff members fulfill internal policies on how they should behave according to privacy policies	Management scrutinizes community interaction data to identify privacy violations
Level 1 scrutiny	Staff members	Staff members monitor laws and ethics concerning privacy concerns	Staff members scrutinize management routines related to privacy, e.g., labor unions protecting staff rights	Staff members scrutinize themselves	Staff members scrutinize community interactions to identify policy violations
Level 0 scrutiny	Community members	Clients monitor laws and ethics concerning privacy concerns	Clients scrutinize community providers' policies and actions related to privacy protection and accountability	Clients scrutinize how staff members intervene in the community	Clients scrutinize their peers and take action to control their own privacy.

Agent Accountability refers to the scrutinization of individuals in their professional roles. At Level 3, it concerns the scrutiny of staff behavior by societal institutions, such as law enforcement (Level 3). At Level 2, it concerns community provider management's monitoring of staff members' privacy behavior concerning internal policies. At subsequent levels, it concerns staff self-scrutinization, such as following checklists (Level 1), and community members' scrutiny of staff interventions in the community (Level 0). What is at stake here is staff members' responsibility regarding community members, their employers, and society.

Finally, *Peer Accountability* refers to the scrutinization of individuals in their role as community members. At Level 3, it concerns the scrutinization of individuals by societal institutions based on direct access to community interaction data. At Level 2, it concerns the scrutiny of community interaction data by community provider management to identify privacy violations. At subsequent levels, it refers to staff members' identification of policy violations (Level 1), and community members' scrutinization of their peers and their own actions to manage privacy regarding themselves (Level 0).

The four modes of scrutiny and their interdependencies outline a systematic protocol for accountability management in an organization. From the community provider point of view, any situation where privacy is breached in Level 1 scrutiny should be justified, in keeping with the policies defined in the organization, should conform to measures required to maintain Level 2 scrutiny, and should be logged for accountability purposes. If a Level 3 scrutiny audit is externally initiated, documentation from Level 2 scrutiny serves as a vital source to account for the organization's actions. What is at stake here is community members' responsibility regarding peers, staff members, community providers, and society.

5.3 Control Flows

On an abstract level, the interdependencies between the levels of scrutiny include (1) the privacy expectations that flow from higher levels to lower levels of scrutiny, and (2) the dynamic information that flows from lower to higher levels, which enables accountability through transparent information use and misuse. We refer to these two flows as the *privacy expectation flow* and the *accountability information flow*. The *privacy expectation flow* signals that stakeholders need to identify and interpret legislation, ethics, and policies at higher levels and communicate these expectations downward. Through their actions, stakeholders and organizational agents then render information traces that constitute the accountability flows that are reported upward. Above, we defined scrutiny as "a process with the ultimate goal to protect privacy while ensuring responsible, accountable use of an information systems artifact. Scrutiny consists of recurring activities and protocols to identify and mitigate the misuse of personal information in an accountable manner." The privacy expectation flow and the accountability information flow are directly related to efficient and effective scrutiny. First, in order to protect privacy ("mitigate misuse"), there is a need for management to facilitate a working flow of privacy expectations. Second, in order to uphold accountability, the accountability information flow must be intact ("an accountable manner").

Our design work in the online psychosocial care setting continually highlights trade-offs between accountability and privacy—an example of conflicting desires between the individual and the community provider. For the organization, there is a need to make balanced and well-informed decisions about when to breach privacy (Belanger & Crossler, 2011). Such decisions made without appropriate reflection jeopardize the community's trust in the organization. Unsolicited breaching of privacy may also be contrary to ethical standards or legislation. Therefore, in addition to scrutinizing what community peers are doing, there is also a need to scrutinize staff behavior. A systematic approach within the organization to govern and manage both Level 1 and Level 2 scrutiny maintains the provider's capabilities to respond to Level 3 scrutiny, i.e., external parties auditing the provider's compliance with legislation and ethics.

In addition to the flows as such, we propose two concepts to support the analysis of scrutiny flows. First, *flow awareness*, which we define as the knowledge within one stakeholder category about the meaning attached to the flow by individuals in the other stakeholder groups. For instance, extensive logging of sensitive information in internal messaging may make sense if it is clear to all why logging occurs (i.e., for accountability reasons) and under what circumstances the data can be accessed, and by whom. Second, *flow disruptions* or "flow flaws," which we define as disturbances in a flow preventing relevant information from propagating to subsequent levels of scrutiny. For instance, a lack of communication of privacy rules from management to staff may lead to different ideas about what "misuse" means, thus disrupting the privacy expectation flow. A "flow flaw" may thus hurt flow awareness. Similarly, a failure to log certain activities may lead to issues in determining accountability. The study of these flow phenomena is an area of ongoing research.

5.4 Scrutiny Design Principles

To generalize our insights on scrutiny, we propose a set of design principles (P1-P4) to set up an effective process of scrutiny for implementation in a system such as U-CARE. In keeping with our definition of scrutiny, the principles aim at supporting an organization in establishing a process that protects privacy by identifying and mitigating the misuse of personal information in an accountable manner. We propose these four principles as ones essential to support design and implementation considerations for the provisioning of scrutiny in information systems. The principles support advice about the design and practical governance of software to facilitate scrutiny of privacy and accountability in organizations. In the practice realm, the ISO/IEC 20510 standard suggests how to assess a set of aspects of accountability issues, which support our findings also from a practical and security perspective. We believe that P1-P4 are necessary design principles, but we do not claim they are sufficient. We look to future research to refine these principles and add new ones. In Section 6, we demonstrate how the Cycle 2 development implemented each of the design principles in the system.

P1: Information Confinement Principle. In order to maintain privacy and accountability, information access should only be permitted within a confined information environment per state-of-the-art security, authentication, and authorization mechanisms in the organization.

P2: Privacy Expectation Principle. In order to satisfy privacy needs at all levels of scrutiny, management should develop and effectively communicate privacy policies in the organization. This design principle supports the *privacy expectation flow* through the levels of scrutiny.

P3: Regulatory and Ethical Compliance Principle. In order to monitor and promote regulatory and ethical compliance in their dealing with information, management should enable a retrospective analysis of stakeholder actions across all levels of scrutiny. This design principle supports the *accountability information flow* through the scrutiny levels.

P4: Breaking the Glass Principle. If privacy is broken, the rationale (and its relation to privacy policies) for "breaking the glass" needs to be documented by the glass breaker (Schefer-Wenzl & Strembeck, 2014). Any single privacy breach should be (1) motivated by the policies defined and communicated following the privacy expectation principle, (2) documented, and (3) followed-up with communications to all stakeholders at Levels 0 to 3.

6 Cycle 2 of the U-CARE System and Scrutiny Evaluation

After a period of reflection that resulted in the formulation of the design theory of scrutiny, we entered Cycle 2 of the software system development and use. During this cycle, the U-CARE system evolved into a software product consisting of three subsystems, ~40,000 lines of code, and ~100 database tables. It has been used in practice by researchers, psychologists, and patients in 11 research trials for three years (April 2013 – September 2016). Approximately 3000 patients have participated in studies using the software. The practical use of the system over three years provides data for a rigorous naturalistic evaluation of the artifact and its use in practice.

Following the Venable et al. (2016) framework for evaluation in design science research (FEDS), we characterize our evaluation as an instance of the *human risk & effectiveness evaluation strategy* (pp. 82-83):

> *The Human Risk & Effectiveness evaluation strategy emphasizes formative evaluations early in the process, possibly with artificial, formative evaluations, but progressing quickly to more naturalistic formative evaluations. Near the end of this strategy more summative evaluations are engaged, which focus on rigorous evaluation of the effectiveness of the artifact, that is, that the utility/benefits of the artifact will continue to accrue even when the artifact is placed in operation in real organizational situations and over the long run, despite the complications of human and social difficulties of adoption and use.*

Our evaluation circumstances provide a rationale for the human risk and effectiveness evaluation strategy: First, we conceive of the significant design risk as social and user oriented. Second, we have seamless access to the practice, making an evaluation based on real use and real data context feasible. Third, we aim at rigorously understanding the enactment and effectiveness of the theory of scrutiny in real situations and over time. Throughout the design process, we conducted formative evaluations following an agile development approach, as reported in Section 4.2. In this section, we account for the summative assessment of the IT system, with a focus on its use and meaning in the U-CARE context. Our evaluation strategy draws its structure from Nunamaker and Briggs (2011). They conceptualize three types of design science research evaluation: Proof of concept (Section 6.1), proof of value (Section 6.2), and proof of use (Section 6.3). Table 3 summarizes the three types of evaluation that we perform during Cycle 2.

Evaluation is a crucial component in DSR research (Hevner et al., 2004). In addition to demonstrating qualities of DSR artifacts, evaluation results provide a basis for assessing the value of the abstract knowledge embodied in the artifact and its practical use (Venable et al., 2016). There is a need to make a distinction between abstract concepts (in this case, ToS) and instantiations (in this case, the U-CARE software and its practical use). Our evaluation efforts highlight the design, use, and value of the instantiated U-CARE software system. ToS is an abstraction that explains the design and provides a rationale for it. There is always a gap between the evaluation results (the merits of the instantiated artifact in the practical setting) and the qualities of the theory that provide a rationale for the design. The proof-of-concept evaluation is more straightforward to account for, since the evaluation is more descriptive, explaining the implementation of technology and planning of practice to match the guidance provided by the principles. The proof-of-value evaluation is less straightforward since it examines the emergence of practice over time and how privacy issues are addressed in the management of that practice. The proof-of-use evaluation also deals with emergence, emphasizing the reception of the software in a broader context.

Table 3. Data Sources for Evaluation

Evaluation type	Data Source(s)	Purpose of evaluation
Proof-of-concept	IT artifact and design process documentation	Demonstrate ToS enactment in practice
Proof-of-value	Management team meeting protocols, policy documents, system logs, backlog data, source code repository (SVN) data	Demonstrate the value of ToS to managerial practice
Proof-of-use	Documentation of ongoing research projects	Demonstrate the pragmatic validity of ToS in a broader practice context

It is possible within the scope of one study to make full connections regarding all three (concept, value, and use). Our evaluations thus demonstrate that ToS (1) resonates with the implementation in the current empirical context (proof of concept), (2) has produced a design that works over time and supports privacy/accountability management in an emerging sociotechnical system (proof of value), and (3) has a pragmatic validity that supports applications both within and beyond the original empirical context (proof of use). A core tenet of pragmatism is that people will embrace concepts and apply those that they find useful. Thus, actual use and dissemination of an idea or an artifact signal its pragmatic validity in practice (Krippendorff, 2005).

6.1 Proof of Concept

The proof-of-concept evaluation in Cycle 2 elaborates on the expanded design of the technical solution and its implementation and use in the U-CARE practice. As presented extensively in Appendix B, the four ToS design principles (Section 5.4) guide our assessment of the feasibility and practical application of the implemented software system.

6.2 Proof of Value

Proof of value is the demonstration of the utility and efficacy of an artifact (Hevner et al., 2004; Nunamaker & Briggs, 2011). To establish proof of value, we conducted a qualitative analysis of management operations in the U-CARE practice. The analysis is based on monthly management team meeting minutes from January 2014 to February 2016 (N=20) imported into nVivo (a software for qualitative analysis). Two of the authors first performed independent open and axial coding (Strauss & Corbin, 1998) of the data to induce two sets of codes and overarching categories. The two researchers then jointly synthesized the induced codes and categories into an agreed-upon set of categories. The result forms the basis for the proof-of-value evaluation. Drawing from management activities in the U-CARE setting, we establish an empirically grounded informed argument (Hevner et al., 2004).

In addition to the analysis of management team minutes, we studied policy documents, system logs, backlog data, and software changes (SVN repository changes and software release data). During the qualitative analysis, two high-level categories emerged, namely *sustained audit practice and institutionalization of scrutiny*. In the following, we address each of these in turn. Anonymized quotes from management team minutes and policy documents were translated from Swedish.

6.2.1 Sustained Audit Practice

The study period (26 months) provided 1875 potential privacy breaches logged in the U-CARE system during the core RCTs. Management scrutinized and audited 1819 of these breaches (the remaining 56 were test data from the process of fine-tuning the software and its use). Breach reports concerning the previous month's breaches were included as a recurring item on the management team meeting agenda. Management formalized the process at an early stage by appointing the scrutiny of privacy breaches to two management roles—the software project lead, X, and the research coordinator, Y: "The steering committee decides that X and Y audit privacy breaches and notify the steering committee if anything is out of the ordinary" (management team protocol, March 12, 2014).

Keeping track of privacy breaches and mitigating misuse of information was considered to be of value in order to identify the rationale for cases of "breaking the glass." Notably, both non-breaches and breaches were relevant to the management team as the confirmation and documentation of non-breaches prepare the organization for external scrutiny audits. Our analysis of steering meeting protocols revealed a three-step audit process for Level 2 Scrutiny that enabled the breaking the glass design principle, as shown in Figure 4.

This process followed the structure of *breach report–measure–closure*. The first step (breach report) occurred when, at a management team meeting, the software project lead or the research coordinator reported any breaches that had occurred over the last month (i.e., since the last meeting): "X reported that psychologist A had retrieved personal information about a person (20

Nov) and that psychologist B at one point (4 Dec) had retrieved personal information about six different persons" (management team protocol, January 13, 2014).

The breach report was always immediately followed by a *measure*—a decision by the management team on how to act on the reported breach: "Y to contact A and B to inquire about the purpose of the personal information retrieval" (management team protocol, January 13, 2014).

For *closure*, measures were followed up at the subsequent management team meeting to ensure that there was an acceptable explanation and that no unresolved issues prevailed: "X reported that the retrieval of personal information from U-CARE by A and B was in the interest of care" (management team protocol, February 12, 2014).

Although the identified audit process contains three distinct steps, it was simplified in cases when enough information for closure was presented already at the time of the breach report, and a separate measure decision was irrelevant: "X reported that C [licensed psychologist] had retrieved personal information related to all participants in ABBA [one of the current studies]" (management team protocol, November 10, 2014).

This breach report was immediately followed by closure since X already had the required information to share, and no further action was needed: "X reported that the retrieval of personal information had been to validate participant information" (management team protocol, November 10, 2014).

A second special case was when a breach report concerned a non-breach, which does not lead to further action but also functioned as closure: "X and Y reported that they had examined the personal information retrieval report for the period 10 Dec 2014 to 15 Jan 2015 and had not noted anything extraordinary" (management team protocol, January 15, 2015).

The establishment of an outlined audit process and its continued enactment by the management team clearly shows that management found considerable value in the ability to report and follow up on privacy breaches, as specified by the ToS and supported by the U-CARE system.

6.2.2 Institutionalization Scrutiny

Our analysis of management minutes revealed that several process changes occurred during the period observed. First, there were changes to improve the efficiency of privacy breach auditing regarding software improvements to facilitate easier management of privacy breach reporting and auditing. For example, management found that several privacy breaches had occurred when support staff helped participants solve logon problems, which resulted in an improvement of the software to better support the auditing of privacy breaches related to support issues. Figure 5 outlines the identified stages of process change.

Based on some particular rationale, a decision was made that resulted in some scrutiny-related changes in the U-CARE practice. Our data analyses identified three distinct areas of institutionalization in addition to software improvements concerned with efficiency and effectiveness of scrutiny activities: *documenting and archiving*, *informing*, and *staffing*. Below, we address these topics in turn.

Documenting and archiving: Several management issues concerned documentation and archiving. From a ToS point of view, such measures concern the removal of disruptions from the accountability flow. First, an example of how new requirements were presented to staff to simplify Level 2 scrutiny: "In order to improve auditing, those who breach privacy from now on will document the rationale for the privacy breach and communicate it to the research coordinator" (management team protocol, March 10, 2014).

Second, management decided that full documentation of privacy breaches should be added to management meeting protocols. The decision built the organization's readiness for Level 3 scrutiny (external audits): "The management team decided that privacy breach audit reports shall be included as appendices to management team meeting protocols" (management team protocol, August 19, 2014).

The audit report specifies privacy breaches and audit results without revealing personal identities (see Table 4 for an excerpt of this report). The design of the report signals management's desire to facilitate sufficient accountability without unjustified use of sensitive information or personal identities. This caution is an attempt at balancing privacy and accountability, which is at the core of ToS.

Informing: Informing staff promoted staff awareness of the policies for accessing personal information. One such measure was to make sure that all associated studies were aware of the implemented scrutiny process: "X is given the task to inform all principal investigators for ongoing associated research trials [names removed] using U-CARE about the steering committee's privacy breach audit process" (management team protocol, May 12, 2014).

On a similar note, to facilitate accountability, it was decided to circulate information to all staff using the U-CARE system about documentation requirements: "The management team decided that information should be sent to staff regarding which documents should be registered and archived, respectively" (management team protocol, September 15, 2014)

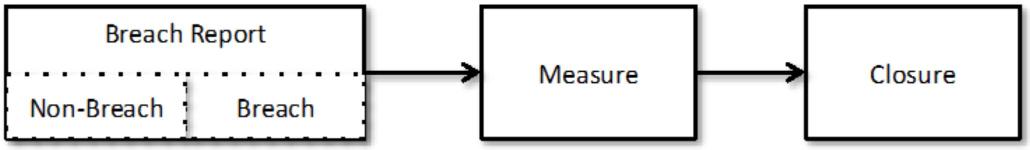

Figure 4. Audit Process in the U-CARE Practice

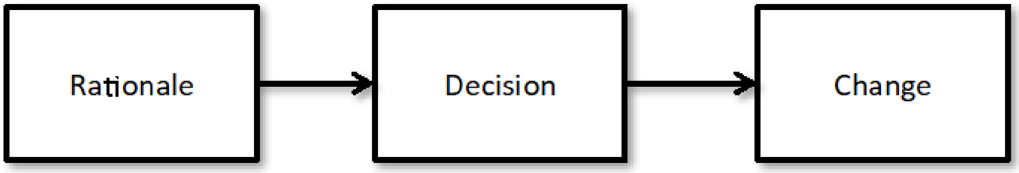

Figure 5. Process Change in the U-CARE Practice

The management team furthermore produced and distributed a series of policy documents to foster scrutiny process compliant behavior (Table 5). Informing, as exemplified here, is central to the privacy expectation flow, i.e., management wanting to make sure that privacy expectations propagate to the staff level. Specifically, all U-CARE policy documents are made publicly available via the internet. From a ToS point of view, this is a manifestation of a dual purpose to both inform staff and to prepare for Level 3 scrutiny by highlighting scrutiny awareness to external auditors.

Staffing: Staffing issues focused on making sure that staff absence should not disrupt the moderation of community activity. An example of this is a concern raised by Y that it should be clarified who would take on his scrutiny tasks should he be unavailable: "Y emphasized that there is a need for routines that secure that audit takes place when he is not present in the workplace" (management team protocol, August 2014)

Further, management noticed that there was a need for technical assistance every time a privacy breach report was needed. Consequently, they decided to remedy the dependency on technicians by building a software feature to view and print breach reports: "The management team decided that the privacy breach log shall be made available through a software feature that does not require technical expertise" (management team protocol, Mar 10, 2014). The requested feature was implemented in June 2014 and has been used since then.

Another staffing issue concerned maintained moderation of participant interaction during holidays: "Since U-CARE operations demand certain staffing during bridging days, we will 'command' staff to be at work these days to ensure that the following functions are represented: psychologist, developer, support, care responsible, and moderator" (excerpt from the policy for holidays and flex time).

6.3 Proof of Use

Proof of use is typically not feasible to demonstrate within a single study since it concerns the "holistic understandings of the rich social, political, economic, cognitive, emotional and physical context in which our systems operate" (Nunamaker & Briggs, 2011, p. 10).While DSR may serve to explore various dimensions of practice, there are limitations to valid claims, given the limited context of use and evaluation. However, we found strong indications about the usefulness of the ToS artifact outside the original scope of design. The pragmatic validity (Hayes & Krippendorff, 2007) of a design refers to the extent to which the design is accepted and adopted by others. In the U-CARE case, several research groups are using the U-CARE system and the ToS protocols in their treatments and research trials (Table 6).

In total, within the research projects shown in Table 6, participants in the studies were recruited at 27 different hospitals in Sweden. eHealth research projects are lengthy, taking into account the time to design and implement technology, designing interventions, acquiring ethical approval, recruiting participants for the studies, conducting the studies, doing post-treatment follow-up studies, and going through journal publication processes. The use of the U-CARE software, which was at the initial idea stage in late 2010, is starting to become visible in research publications. Early papers concern the design of internet-based trials (e.g., Mattsson et al., 2013; Norlund et al., 2015; Ander et al., 2017; Hauffman et al., 2017). More recent papers report on trial results (e.g., Larsson et al., 2017; Ternström et al., 2017; Norlund et al., 2018; Wallin et al., 2018; Hauffman et al., 2020a; Hauffman et al. 2020b) and studies of user behavior in eHealth contexts (e.g., Wallert et al., 2018; Igelström et al., 2020).

Table 4. Excerpt from the Privacy Audit Report of December 2014

Timestamp	Staff user	Participant user ID	Study	Audit status	Audited by
2014-12-04 12:46	Claes	Nn	Applied Relaxation C	Journal	Inga
2014-12-02 09:32	Greta	Nn	ISAK - KBT	Support	Inga
2014-12-01 16:28	Greta	Nn	U-CARE: Heart	Support	Inga
2014-12-01 11:31	Greta	Nn	ISAK - KBT	Support	Inga
2014-12-01 11:29	Greta	Nn	ISAK - KBT	Support	Inga
2014-12-01 11:25	Greta	Nn	U-CARE: Adults with Cancer	Support	Inga

Table 5. Policy Documents

Policy Document	Scrutiny focus	ToS institutionalization
Work task descriptions	Delegation of responsibility	Ensuring responsibility for level 2 scrutiny.
Off-premises data management	Use of research and treatment data outside the workplace	Supporting scrutiny process compliance in a distributed work environment
Holidays and flex time	Maintaining the integrity of level 2 scrutiny	Matching scrutiny demands with employment regulations
Publicity and confidentiality	General principles for staff use of sensitive and confidential data	Ensuring privacy expectations are explicitly articulated in the organization

Table 6. Research Trials Using U-CARE Software

Research Trial	Period	#Participants
RCT investigating the efficacy of a psychosocial health intervention for adults with cancer	Apr 2013 – Sep 2016	1057
RCT investigating the efficacy of a psychosocial health intervention for adults who suffered a myocardial infarct.	Sep 2013 – Sep 2016	914
RCT comparing two different methods for treating fear of childbirth in pregnant women.	Mar 2014 – Apr 2016	270
RCT investigating the efficacy of a psychosocial health intervention for patients with pelvic pain.	Mar 2014 – Aug 2016	175
RCT studying the effect of relapse prevention for people who take anti-depressive medication but who still show residual symptoms.	Jan 2014 – Jan 2016	105
Two connected RCTs comparing how a varied degree of therapeutic support and variations in multimedia richness affects adherence to treatment.	Apr – Dec 2014, Feb – Oct 2016	185 + 100
Two connected RCTs examining the effect of CBT online to help women and couples cope better after having negative or traumatic experiences in connection with childbirth.	Mar 2014 – Sep 2016	235 + 39
Participatory action research to inquire into the needs for psychosocial support among parents with cancer-struck adolescents.	May 2016	6
Qualitative inquiry into teenage impressions of online psychosocial care and supporting technologies.	Dec 2012 – Mar 2015	9

The extensive use of the software outside the original context of design provides clear evidence supporting the effectiveness of U-CARE and the theory of scrutiny. We make the following observations on the actual use of U-CARE in research trials:

First, adoption of the software outside the design context does not guarantee that the adopters profoundly reflected on the quality of the software support for “scrutiny” and the mitigation of misuse. However, they *have* adopted the software. This adoption means that they have not chosen to reject the software based on their conception of its scrutiny features. We presume that they, as psychology researchers, consider privacy threats and information management to be crucial issues in their research. Thus, the researchers found the design sufficient to conduct their trials.

Second, software adoption is not only related to software features but also other factors impacting trust in the software. Presumably, the multi-disciplinary researchers’ trust in the U-CARE practice affected their choice to adopt the software to support their research. While trust is a complex issue, we argue that, for the management practices of U-CARE, continually focusing on privacy issues has had a vital function in building trust. Other research groups have accepted not only the software but also the U-CARE practice in their process of deciding whether or not to adopt the software. This line of reasoning implies that the way that U-CARE-management enacted ToS has helped build trust in the research community.

Third, each associated study has gone through an ethical approval process. The ethical approval applications used an early version of the description of the implementation of the information confinement principle described in Section 5.4. The ethical approval board concluded that there was a sufficient level of privacy in the design at hand. We consider the ethical approval of the additional trials as prima facia evidence supporting the theory of scrutiny.

7 Discussion and Future Research Directions

In this paper, we draw on our experiences in performing software systems design in the domain of online psychosocial care. Following Baskerville et al. (2018), this DSR effort contributes technologically and theoretically in a balanced manner. On a technological level, we contribute: (1) an innovative artifact in the form of the U-CARE sociotechnical system for the provision and study of psychosocial care. An instantiated IT artifact is theory made concrete (Baskerville et al., 2018). The U-CARE platform also provides the functionality for clinical trials of the delivered CBT treatments. We also contribute (2) an innovative action framework (a process model) used in the development of the U-CARE system, as described in Section 4.

On a theoretical level, we contribute (1) situated definitions of the constructs *privacy, accountability*, and *scrutiny* in the application area of eHealth; and (2) a *design theory of scrutiny* with three focal components (presented in Section 5): namely, the scrutiny protocol matrix, two scrutiny control flows, and four scrutiny design principles. We thus provide *technological* contributions consisting of a rich depiction of a process of designing for privacy and accountability, a software system design, and a naturalistic evaluation of the U-CARE system enacted in practice.

We also assert *theoretical* contributions surrounding the design theory of scrutiny. The current study is the first comprehensive, longitudinal DSR study to develop and evaluate a design theory for the development of sensitive online healthcare systems. The theory addresses the relationships between accountability and privacy, explaining how these concepts relate to the interdependency among four groups of system stakeholders and four layered levels of scrutiny. We propose a representation of the theory in the form of a multilayered protocol that assigns clear responsibilities among peers, agents, management, and external (societal) stakeholders in an online community. The protocol supports a fuller understanding of the two critical flows of privacy expectations and accountability and their points of communication and potential disruption. We propose four fundamental scrutiny design principles to support the provisioning of scrutiny in sensitive information systems in order to identify and mitigate the misuse of personal information in an accountable manner. The principles advocate the necessity of a confined information environment, nondisrupted privacy expectation, accountability compliance flows, and privacy breaches only when justified by organizational policy founded in regulations and ethics.

High privacy expectations among patients, governed by the professional ethics of psychologists, characterized the online psychosocial care context studied in this research. Therefore, it is not surprising that the scrutiny process in the U-CARE practice was accepted without protest. Future research should explore the reception of a rigorous scrutiny process in other contexts that are less accustomed to systematic monitoring.

By demonstrating and evaluating the particular implementation of the theory in the current empirical setting, as suggested by Venable et al. (2016), we signal the value of the abstract knowledge (i.e., design theory of scrutiny) embodied in the software artifact and practice. We demonstrate the qualities of the theory through a three-faceted evaluation. First, proof of concept, showing the implementation of the theory through the design of technology and organizational practice. Second, proof of value, showing how practice enacts the theoretical concepts. We argue that the sustained audit practice, the institutionalization of scrutiny, and scrutiny process improvements—in line with ToS—serve as evidence of its value for the organization. Third, proof of use, where we demonstrate how the U-CARE software and associated practices have been adopted outside its context of origin, demonstrating to some degree the pragmatic validity of the design theory of scrutiny.

Regarding research limitations, the current version of the theory is a generalization from a single case study (Lee & Baskerville, 2003). The U-CARE system supports both the practice of online psychosocial care and research into such care. Uppsala University registered as a healthcare provider to conduct the trials. Consequently, the privacy and accountability experiences justifying ToS have emerged through a design process addressing compliance with healthcare provision legislation as well as research legislation and ethics. The current empirical setting—online psychosocial care—served us well in exploring the issue at hand because of the intensive use of sensitive information and regulatory complexity.

ToS should be seen as a set of privacy- and accountability-focused concepts to support structured thinking about privacy and accountability. The theory does not presume any particular legislative or ethical framework but needs such a framework in place to be effectively implemented. Furthermore, in a practical design situation, ToS should be used together with appropriate state-of-the-art information security concepts. For instance, the information confinement principle promotes the identification and mitigation of inappropriate access to sensitive data by database administrators and hackers. However, it does not prescribe exactly how to achieve such managerial governance and assumes integration with technical knowledge from relevant fields, such as network communications, IT security, information security, and database management.

It is easy to think of settings beyond psychosocial care where a community provider might need to relate to both accountability and privacy. We argue that ToS would make a useful foundation for inquiries into other types of online communities, such as e-learning (e.g., MOOCs), online news, criminology, citizen dialogues in e-government practices, and scholarly peer review. Each of these settings relies on specific legislative and ethical governance frameworks, but community providers in these settings likely face situations similar to U-CARE in terms of an environment exposed to and threatened by social and technical vulnerabilities, which resonates with the purpose and scope of the theory. We also posit that despite stemming from an eHealth context, the ToS concepts may provide an exciting and relevant lens to study privacy issues that online social networks, such as Facebook and Twitter, are currently addressing (not least in the aftermaths of the recent US election).

U-CARE software, as an implementation of ToS principles, provides a foundation for analyzing and visualizing behavior related to privacy and auditing. The design of the audit process affects the behavior of auditors, e.g., their monthly management meeting affected the use of the software to audit privacy breaches. To the best of our knowledge, this is the only design theory that comprehensibly explains scrutiny in the context of online information systems and that also proposes concrete guidelines and an expository instantiation for its implementation in software and enactment in practice.

Acknowledgments

We thank our colleagues working in or close to the U-CARE program. This work was supported by The Swedish Research Council (2009-1093). We acknowledge the insightful comments of the editors and reviewers that led to many improvements in the final paper.

References

Aakhus, M., Ågerfalk, P. J., Lyytinen, K., & Te'eni, D. (2014). Symbolic action research in information systems: Introduction to the Special Issue. *MIS Quarterly*, *38*(4), 1187-1200.

Ågerfalk, P. J. (2014). Insufficient theoretical contribution: A conclusive rationale for rejection? *European Journal of Information Systems*, *23*(6), 593-599.

Ågerfalk, P. J. (2020). Artificial intelligence as digital agency. *European Journal of Information Systems*, *29*(1), 1-8.

Ågerfalk, P. J., & Eriksson, O. (2004). Action-oriented conceptual modelling. *European Journal of Information Systems*, *13*(1), 80–92.

Ågerfalk, P. J. (2018). Whither design science research? *European Journal of Information Systems*, *27*(2), 127-128.

Ågerfalk, P., & Karlsson, F. (2020). Artefactual and empirical contributions in information systems research. *European Journal of Information Systems*, *29*(2), 109-113.

Ander, M., Wikman, A., Ljótsson, B., Grönqvist, H., Ljungman, G., Woodford, J., ... & von Essen, L. (2017). Guided internet-administered self-help to reduce symptoms of anxiety and depression among adolescents and young adults diagnosed with cancer during adolescence (U-CARE: YoungCan): a study protocol for a feasibility trial. *BMJ Open*, *7*(1), Article e013906.

Barak, A., Hen, L., Boniel-Nissim, M., & Shapira, N. (2008). A comprehensive review and a meta-analysis of the effectiveness of internet-based psychotherapeutic interventions. *Journal of Technology in Human Services*, *26*(2-4), 109-160.

Baskerville, R. & Myers, M. (2004). Special issue on action research in information systems: Making IS research relevant to practice. *MIS Quarterly*, *28*(3), 329-336.

Baskerville, R. & J. Pries-Heje (2010). Explanatory design theory. *Business & Information Systems Engineering*, *2*(5), 271-282.

Baskerville, R., Kaul, M. & Storey, V.C. (2015). Genres of Inquiry in Design-Science Research: Justification and Evaluation of Knowledge Production. *MIS Quarterly*, *39*(3), 541-564.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design Science Research Contributions: Finding a Balance between Artifact and Theory. *Journal of the Association for Information Systems*, *19*(5), 358-376.

Bélanger, F. & Crossler, R. E. (2011). Privacy in the Digital Age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041.

Burton-Jones, A., Recker, J., Indulska, M., Green, P., & Weber, R. (2017). Assessing representation theory with a framework for pursuing success and failure. *MIS Quarterly*, *41*(4), 1307-1333.

Cronen, V. (2001). Practical theory, practical art, and the pragmatic-systemic account of inquiry. *Communication Theory*, *11*(1), 14-35.

Culnan, M. (2003). Consumer privacy, technology and policy. In J. F. George (Ed.), *Computers in society: Privacy, ethics and the internet* (pp. 171-183). Pearson/Prentice Hall.

Dance, G., LeForgia, M. & Confessore, N. (2018, December 18). As Facebook raised a privacy wall, it carved an opening for tech giants. *The New York Times*. https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html

Dewey, J. (1938). *Logic: The theory of inquiry*. Henry Holt.

Eriksson, O., Johannesson, P., & Bergholtz, M. (2018). Institutional ontology for conceptual modeling. *Journal of Information Technology*, *33*(2), 105-123.

Garfinkel, H. (1967). *Studies in ethnomethodology*. Polity Press.

Goldkuhl, G. (2004). Design theories in information systems: A need for multi-grounding. *Journal of Information Technology Theory and Application*, *6*(2), Article 7.

Goldkuhl, G. & Ågerfalk, P. J. (2005). IT Artefacts as socio-pragmatic instruments: Reconciling the pragmatic, semiotic, and technical. *International Journal of Technology and Human Interaction*, *1*(3), 29-43.

Goldkuhl, G. & Lind, M. (2010). A multi-grounded design research process. In R. Winter, L. Shao, & S. Aier (Eds.), *Global perspectives on design science research: Proceedings of DESRIST* (pp. 45-60).

Gregor, S. (2006). The Nature of Theory in Information Systems, *MIS Quarterly*, *30*(3), 611-642.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, *37*(2), 337-355.

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, *8*(5), 312-335.

Grönqvist, H., Olsson, E. M. G., Johansson, B., Held, C., Sjöström, J., Norberg, A. L., Hovén, E., Sanderman, R., van Achterberg, T., & von Essen, L. (2017). Fifteen challenges in establishing a multidisciplinary research program on eHealth research in a university setting: a case study. *Journal of Medical Internet Research*, *19*(5), Article e173.

Hassan, N. R., Mathiassen, L., & Lowry, P. B. (2019). The process of information systems theorizing as a discursive practice. *Journal of Information Technology*, *34*(3), 198-220.

Hauffman, A., Alfonsson, S., Mattsson, S., Forslund, M., Bill-Axelson, A., Nygren, P., & Johansson, B. (2017). The development of a nurse-led internet-based learning and self-care program for cancer patients with symptoms of anxiety and depression: A part of U-CARE. *Cancer Nursing*, *40*(5), E9-E16.

Hauffman, A., Alfonsson, S., Bill-Axelson, A., Bergkvist, L., Forslund, M., Mattsson, S., von Essen, L., Nygren, P., Igenström, H. (2020a). Co-created internet-based stepped care for individuals with cancer and concurrent symptoms of anxiety and depression: Results from the U-CARE AdultCan randomized controlled trial. *Psycho-Oncology*, 29(12), 2012-2018.

Hauffman, A., Alfonsson, S., Igelström, H., & Johansson, B. (2020b). Experiences of internet-based stepped care in individuals with cancer and concurrent symptoms of anxiety and depression: Qualitative exploration conducted alongside the U-CARE AdultCan randomized controlled trial. *Journal of Medical Internet Research*, *22*(3), Article e16547.

Hayes, A. & Krippendorff, K. (2007). Answering the call for a standard reliability measure for coding data, *Communication Methods and Measures*, *1*(1), 77-89.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105.

Hevner, A. (2007). A three cycle view of design science research, *Scandinavian Journal of Information Systems*, *19*(2), 87-92.

Igelström, H., Hauffman, A., Alfonsson, S., Sjöström, J., Cajander, Å., & Johansson, B. (2020). User experiences of an internet-based stepped-care intervention for individuals with cancer and concurrent symptoms of anxiety or depression (the U-CARE AdultCan Trial): Qualitative study. *Journal of Medical Internet Research*, *22*(5), Article e16604.

Iivari, J. (2014). Distinguishing and contrasting two strategies for design science research. *European Journal of Information Systems*, *24*(1), 107-115.

Iivari, J. (2020). A Critical look at theories in design science research. *Journal of the Association for Information Systems*, *21*(3), 502-519.

Kordzadeh, N. & Warren, J. (2017). Communicating personal health information in virtual health communities: An integration of privacy calculus model and affective commitment, *Journal of the Association for Information Systems*, *18*(1), 45-81.

Krippendorrf, K. (2005). *The semantic turn: A new foundation for design*. CRC Press.

Kuechler, B. & Vaishnavi, V. (2008). On theory development in design science research: Anatomy of a research project. *European Journal of Information Systems*, *17*(5), 489-504.

Larsson, B., Karlström, A., Rubertsson, C., Ternström, E., Ekdahl, J., Segebladh, B., & Hildingsson, I. (2017). Birth preference in women undergoing treatment for childbirth fear: A randomized controlled trial. *Women and Birth*, *30*(6), 460-467.

Lee, A. S., & Baskerville, R. (2003). Generalizing Generalizability in Information Systems Research. *Information Systems Research*, *14*(3), 221-243.

Lukyanenko, R., & Parsons, J. (2020). Design Theory Indeterminacy: What is it, how can it be reduced, and why did the polar bear drown? *Journal of the Association for Information Systems*, *21*(5), 1343-1369.

March, S. T., & Allen, G. N. (2014). Toward a social ontology for conceptual modeling. *Communications of the Association for Information Systems*, *34*, 1347-1358.

Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A Design theory for systems that support emergent knowledge processes, *MIS Quarterly*, *26*(3), 179-212.

Mattsson, S., Alfonsson, S., Carlsson, M., Nygren, P., Olsson, E., & Johansson, B. (2013). U-CARE: Internet-based stepped care with interactive support and cognitive behavioral therapy for reduction of anxiety and depressive symptoms in cancer: A clinical trial protocol. *BMC Cancer*, *13*(1), Article 414.

Mitnick, K. & Vamosi, R. (2017). *The Art of invisibility*. Little, Brown, & Co.

Mustafa, M. I. (2019). *Sustaining the usefulness of ehealth research software: Lessons learned in action design research* [Doctoral dissertation, Uppsala University].

Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital innovation management: reinventing innovation management research in a digital world, *MIS Quarterly*, *41*(1), 223-238.

Norlund, F., Olsson, E. M., Burell, G., Wallin, E., & Held, C. (2015). Treatment of depression and anxiety with internet-based cognitive behavior therapy in patients with a recent myocardial infarction (U-CARE Heart): Study protocol for a randomized controlled trial. *Trials*, *16*(1), 1-8.

Norlund, F., Wallin, E., Olsson, E. M. G., Wallert, J., Burell, G., von Essen, L., & Held, C. (2018). Internet-based cognitive behavioral therapy for symptoms of depression and anxiety among patients with a recent myocardial infarction: the U-CARE heart randomized controlled trial. *Journal of Medical Internet Research*, *20*(3), Article e88.

Nunamaker, J. F., & and Briggs, R. O. (2011). Towards a broader vision for information systems. *ACM Transactions on Management Information Systems*, 2(4), Article 20.

Nunamaker, J. F., Twyman, N. W., Giboney, J. S., & Briggs, R. O. (2017). Creating high-value real-world impact through systematic programs of research. *MIS Quarterly*, *41*(2), 335-251.

Parker, G., Van Alstyne, M., & Choudary, S. (2016). *Platform revolution: How networking markets are transforming the economy and how to make them work for you*. Norton.

Riley, S., & Veale, D. (1999). The internet & its relevance to cognitive behavioural psychotherapists. *Behavioural and Cognitive Psychotherapy*, *27*(1), 37-46.

Schefer-Wenzl, S. & Strembeck, M. (2014). Model-driven specification and enforcement of RBAC break-glass policies for process-aware information systems, *Information and Software Technology*, *56*, 1289-1308.

Scrum Alliance. (2018). *2017-18 State of Scrum report*: *Scaling and agile transformation*. https://www.scrumalliance.org/learn-about-scrum/state-of-scrum/2018-state-of-scrum.

Searle, J. R. (1969). *Speech acts: An essay in the philosophy of language*. Cambridge University Press.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS Quarterly*, *35*(1), 37-56.

Sjöström, J. (2010). *Designing information systems: A pragmatic account* [Doctoral dissertation, Uppsala University].

Sjöström, J., Alfonsson, S. (2012). Supporting the therapist in online therapy. *Proceedings of the European Conference on Information Systems.*

Sjöström J., Ågerfalk P. J., & Hevner A. (2014). A multi-layer scrutiny protocol for privacy and accountability. *Proceedings of DESRIST*. Springer.

Sjöström, J., von Essen, L., & Grönqvist, H. (2014). The origin and impact of ideals in eHealth research: Experiences from the U-CARE research environment. *JMIR Research Protocols*, *3*(2), Article e28.

Sjöström J., Ågerfalk P. J., & Hevner, A. (2017). Scrutinizing privacy and accountability in online psychosocial care, *IEEE IT Professional*, *19*(3), 45-51.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1015.

Strauss, A.L. & Corbin, J.M. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (2nd ed.) SAGE.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology and Behavior*, *7*(3), 321-327.

Sutton, R. I. & Staw, B. M. (1995). What theory is not. *Administrative Science Quarterly*, *40*(3), 371-384.

Tate, D., & Finkelstein, E. (2009). Cost effectiveness of internet interventions: review and recommendations. *Annals of Behavioral Medicine*, *38*(1), 40-45.

Ternström, E., Hildingsson, I., Haines, H., Karlström, A., Sundin, Ö., Ekdahl, J., ... & Rubertsson, C. (2017). A randomized controlled study comparing internet-based cognitive behavioral therapy and counselling by standard care for fear of birth-a study protocol. *Sexual & Reproductive Healthcare*, *13*, 75-82.

Thorén, C., Ågerfalk, P. J., & Edenius, M. (2014). Through the printing press: An account of open practices in the Swedish newspaper industry. *Journal of the Association for Information Systems*, *15*(11), 779-804.

United Nations. (1948). *The universal declaration of human rights*. https://www.un.org/en/universal-declaration-human-rights/index.html

Vance, A., Lowry, P., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of MIS*, 29(4), 263-290.

Vance, A., Lowry, P., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, *39*(2), 345-366.

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A framework for evaluation in design science research. *European Journal of Information Systems*, *25*(1), 77-89.

Wainer, J., Kumar, A., & Barthelmess, P. (2007). DW-RBAC: A formal security model of delegation and revocation in workflow systems. *Information Systems*, *32*(3), 365-384.

Wallert, J., Gustafson, E., Held, C., Madison, G., Norlund, F., von Essen, L., & Olsson, E. M. G. (2018). Predicting adherence to internet-delivered psychotherapy for symptoms of depression and anxiety after myocardial infarction: Machine learning insights from the U-CARE Heart Randomized Controlled Trial. *Journal of Medical Internet Research*, *20*(10), Article e10754.

Wallin, E., Norlund, F., Olsson, E. M. G., Burell, G., Held, C., & Carlsson, T. (2018). Treatment activity, user satisfaction, and experienced usability of internet-based cognitive behavioral therapy for adults with depression and anxiety after a myocardial infarction: Mixed-methods study. *Journal of Medical Internet Research*, *20*(3), Article e87.

Walls, J., Widmeyer, G., and El Sawy, O. A. (1992). Building an information systems design theory for vigilant EIS. *Information Systems Research*, *3*(1), 36-59.

Weber, M. (1978). *Economy and society: An outline of interpretive sociology* (vol. 1). Univ of California Press.

Weick, K. E. (1995). What theory is not—theorizing is. *Administrative Science Quarterly*, *40*(3), 385-390

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Communications of the ACM*, *51*(6), 82-87.

Zhuo, J. (2010). Where anonymity breeds contempt. *The New York Times*. https://www.nytimes.com/2010/11/30/opinion/30zhuo.html.

Appendix A

In this appendix, we elaborate on our view on theorizing in DSR. We expand the underlying pragmatist perspective on theory and the notion of multigrounded theory for knowledge justification.

A.1 A Pragmatist Perspective on Design Theory

Reflections on DSR contributions provide an essential starting point for the use of DSR methods in theory development (Walls et al., 1992; Gregor & Jones, 2007; Kuechler & Vaishnavi, 2008; Baskerville & Pries-Heje, 2010; Gregor & Hevner, 2013; Iivari, 2014). The consensus seems to be that design theory is the result of learning and generalization from the evaluation of an artifact whose design is predicated on a set of kernel theories. This relationship can be depicted as: kernel theories → artifact (build and evaluate) → design theory (*in situ* validated kernel theory). For example, Hevner et al. (2004, p. 76), citing Markus et al. (2002) and Walls et al. (1992), state that the creation of DSR artifacts "relies on existing kernel theories that are applied, tested, modified, and extended through the experience, creativity, intuition, and problem solving capabilities of the researcher."

In keeping with pragmatism, the main philosophical foundation of DSR (Hevner et al., 2004), we conceive of design theory as a practical means to aid inquiry. Inquiry, as accounted for by Dewey (1938), encompasses both design and evaluation and aims at changing an unwanted situation into a preferred one. Thus, an inquiry into privacy management, for instance, could be conducted to understand and resolve problematic issues in current privacy management practice. Drawing on Dewey's (1938) stages of inquiry, Cronen (2001, p. 29) summarizes the idea of a "practical theory" by stating that a theory is practical if it is useful for "(1) identifying a situation-in-view, (2) constructing judgments (systemic hypotheses) that (3) implicate actions leading to (4) the consequence of improving the situation." Thus, a practical theory directly addresses the problem of design theory indeterminacy (i.e., the link between theoretical constructs and artifactual constructs and practices) as discussed by Lukyanenko and Parsons (2020).

While design theory in IS (e.g., Gregor & Jones, 2007) addresses a solution to a class of problems, the notion of a practical theory suggests that situated inquiry into current practice is an integrated part of a design initiative. A practical theory may be composed of elements that correspond to Type IV (explanation and prediction) and Type V (design and action) in Gregor's (2006) taxonomy of theory types in information systems. As such, it is not necessarily a design theory in the Gregor and Jones (2007) sense but closer to what Iivari (2020) calls design knowledge as the result of formalized learning in a design research process (Sein et al., 2011). To be considered practical, a theoretical DSR contribution must relate to a specific technological/artifactual contribution (Baskerville et al., 2018; Ågerfalk & Karlsson, 2020). Thus, our theory development approach does not aim for deductively validated hypotheses but for theoretically and empirically justified propositions: kernel theory ↔ multi-grounded practical design theory ↔ artifact (and its application).

A.2 Theory Justification through Multigrounding

We characterize the theory of scrutiny (ToS) as a multigrounded theory (Goldkuhl, 2004; Goldkuhl and Lind, 2010) justified through three grounding processes: Empirical grounding, theoretical grounding, and internal grounding. These processes concern both the context of discovery and the context of justification through "the researcher's subjective thinking processes and the discursive activities that follow … [and] the same researcher's 'rational reconstructions." (Hassan et al., 2019, p. 200)

Empirical grounding relates to the DSR relevance cycle, as outlined by Hevner (2007). In DSR, empirical grounding is an interactive process concerned with both designed artifacts and design knowledge expressed as design theory. Theories leave traces in designed artifacts, which are built and evaluated empirically. Empirical observations (domain understanding) also feed into the design research process, which formalizes learning as design theory. In the U-CARE project, over 100 design workshops involved a wide range of stakeholders during the software design process, promoting the relevance of the design and its rationale. The design workshops factored user requirements as well as legislation and ethical standards into the design process. All nine clinical trials conducted via the software have undergone ethical approval, including auditing of the management of information use and privacy in the U-CARE practice. The empirical grounding also includes evaluation based on logged data and experiences from using the software in a real-world setting.

Theoretical grounding relates to the rigor cycle in DSR (Hevner 2007). ToS has evolved through cycles of studies of the knowledge base. In keeping with Gregor and Hevner (2013), DSR not only serves to develop knowledge about the solution but also to increase the conceptual understanding of the problem domain. Throughout the project, the appreciation of the problem domain has emerged, pointing out the need for further inquiry into the knowledge base to feed continued theoretical abstraction. We conceive of design as a search process not only to create a "solution," but also a search for a better understanding of the problem as such (Ågerfalk, 2014).

Third, *internal grounding* refers to the logical coherence between propositions in the emerging theory. New empirical and theoretical findings may contradict one another or illuminate previously unknown phenomena. Such situations call for reflection and reformulation of theoretical propositions to promote the explanatory power of the theory and the internal coherence between its constructs.

We agree with Sutton and Staw (1995) that data, references, lists of variables, models, and stand-alone hypotheses do not constitute theory per se. The multigrounded approach to theorizing through DSR is a rigorous interim struggle towards justified theory (cf. Weick, 1995). It is a discursive practice of consideration through abductive inferences that emphasizes a balance between the contexts of discovery and justification (Hassan et al., 2019).

While the current study draws from a single case, we expect subsequent research to further elaborate ToS and contribute to the understanding of the problem domain as well as provide alternatives for how to manage scrutiny in organizations.

Appendix B: Evaluation of Design Principles in the U-CARE Software System

As a proof-of-concept evaluation of the U-CARE system in Cycle 2, we discuss the impacts of the scrutiny design principles in the implemented system.

B.1 Implementation of the Information Confinement Principle

Accessing information outside the confined environment introduces the risk that information falls into the wrong hands (privacy threat), and also that the organization does not record the access to that information (lack of accountability). That is, there is a risk for misuse that cannot be identified or mitigated. Information confinement is implemented through the provision of general security mechanisms, separation of data, reflected logging mechanisms, and minimal use of nonsecure channels.

- *General security mechanisms.* The software implementation was governed by Swedish regulation, in keeping with European Union directives on the processing of personal and sensitive information, requiring standard measures to encrypt storage and communication of information. A two-pass authentication scheme (username and password followed by entering a code sent by SMS to the user) ensures compliance with legislation for online health systems. As seen in Figure B1, all software is protected by a firewall that only accepts requests to the ports managing the encrypted web requests. The separation mechanisms allow for multiple security measures to limit the access to Server 2: (1) IP restrictions (requests are only allowed from Server 1 to Server 2), (2) a limited API is offered from the Personal data service to the Web portal, and (iii) all requests from the Web portal to the Personal data service are logged to facilitate retrospective analyses of data access. That is, any access of personal data would "break the glass" (see also Section B.4 below).
- *Separation of data.* To reduce the risk of identifying individuals, personal data, and user-generated content is stored in different databases (see Figure B1). A limited number of system administrators can access both databases—all of whom are bound by nondisclosure agreements to prevent misuse of information. The lead researcher in each clinical study is allowed to extract user-generated data and connect it to identified individuals when the data collection phase of a study has ended. The deanonymization of data is part of each study's design and approved by a research ethical approval board. Study participants are informed about the data collection and data processing procedure when they give their consent to be part of a study.
- *Reflected logging mechanisms.* The web is a complex infrastructure for distributed information processing. Third parties operating in this infrastructure may pose security threats, e.g., by creating additional layers of logging on top of what the organization logs. Overly extensive logging may in itself be a threat to privacy. As an example, a web server or an internet service provider may have a default setting to keep its request logs, including IP addresses. The content of such a record may be valuable for usage statistics, etc., but it may also be a source of misuse of information. In the U-CARE software, logging is done within the confined environment, as outlined in Figures 2 and 3 of the paper. However, some exceptions were made during limited periods to deal with performance issues and bugs.
- *Minimal use of nonsecure channels.* Channels such as email and SMS to external parties may be valuable in software design, but they are likely to be insecure. The software contains several functions that allow staff to configure how to send SMS and email reminders to participants. It was also decided that such reminders should never include sensitive information.

B.2 Implementation of the Privacy Expectation Principle

The U-CARE practice incorporates privacy expectations and privacy expectation flows in various ways: First, *privacy intelligence* deals with how the organization monitors and adapts its policies to the societal privacy discourse. Second, *privacy expectation dissemination* activities communicate privacy policies to actors in the organization. Third, the implemented system incorporates *software manifestations of privacy expectations* throughout its design. We elaborate further on these three aspects of privacy below.

- *Privacy intelligence.* During the design process, significant resources were invested in understanding privacy ethics and legislation, including discussions with ethical approval boards and government agencies. These initial understandings informed software design as well as policymaking. There is no dedicated continuous process to monitor changes in privacy legislation. Instead, the evolved understanding of societal privacy expectations in U-CARE is a result of general design activities and ethical approval applications. Typically, when there are requests for changes in processes or software, privacy issues are discussed in the management team. If the changes may be threats to privacy, further inquiry investigates the matter before implementing any changes in policies or the live software environment.

- *Privacy expectation dissemination.* Several policy documents in U-CARE manifest privacy expectations, including (1) consent forms signed by individuals before they become participants in a study, (2) "netiquette" rules that are shown to participants, explaining the expected behavior among community peers, and (3) the moderator manual (excerpted in Table B1) that is used by staff, consisting of guidelines that regulate when privacy may be breached. Psychologists, researchers, and health staff developed the manual. In total, it consists of 15 anomalies, including pornographic content, insults, hate speech, advertising, propaganda, etc. These anomalies represent four categories: Rule violations, medical/therapeutic claims without or contradictory to evidence, negative spirals, and destructive tendencies. Explicit rules for privacy breaches serve as instruments for balancing privacy and accountability requirements. In this case, the organization's goal is to offer an anonymous environment that should promote people's health and healthy behavior. Each anomaly should be understood as a deviation from what is desirable based on a stakeholder's responsibility. The abnormality may lead to undesired consequences for stakeholders. The negative spirals, for example, may lead to less healthy behavior, which contradicts the organization's goals as a caregiver.

Figure B1. Separation of Data

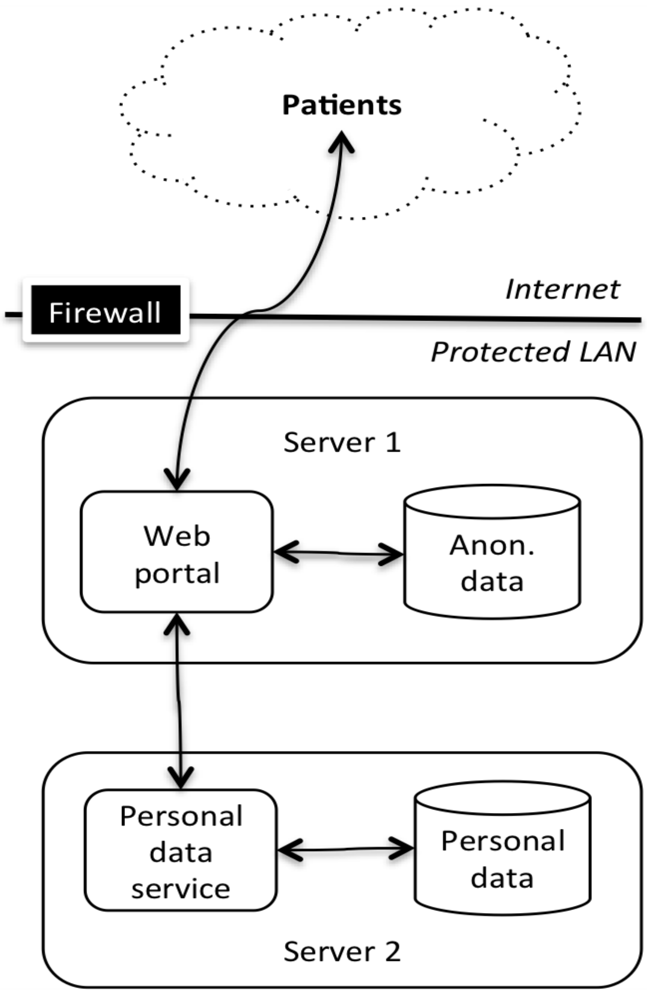

Table B1. Excerpt from the “Moderator Manual.”

Anomaly	Example	Corrective action(s)
Self-destructive or violent tendencies	A discussion revolves around self-destructive or suicidal thoughts.	Immediately contact the responsible therapist(s), who will, in turn, breach privacy to get in touch with the patient(s). Remove the content.
Respect for others	A public discussion exposes the real name of another participant.	Remove the content with a comment on why. Write an internal message to the subject stating that it is not allowed to reveal the identity of other participants.
Promotion of illegal activity	A patient recommends illegal drugs and how to purchase them on the Internet.	Remove the content. Send an internal message to the subject, informing that illegal activities may not be promoted in the community. Contact the police in case there is reason to believe that someone is in danger.

B.3 Implementation of the Regulatory and Ethical Compliance Principle

The accountability flow, as embodied in this principle, has had a significant impact on software design as well as business processes. The logging mechanism, as shown in Figures 2 and 3 of the paper, is an essential foundation to support regulatory and ethical compliance. The system logs serve as a critical data source to analyze past actions in the community among participants, staff, and management. Compliance implementation occurs at all four scrutiny levels.

Peer self-scrutiny (Level 0 scrutiny) occurs in the community. Participants are allowed to tailor their visibility in the community and block other users from communicating with them. The default is that users are invisible to others - they need to make an active choice to become visible. Further, the feature to report forum posts that do not comply with privacy expectations is an example of peer self-scrutiny.

Staff moderation of the community (Level 1 scrutiny) is supported through a “community monitor view,” in which staff can filter community peer interaction. The intended workflow is that each study requires staff to enter this view daily and audit all communication between peers. A rudimentary algorithm for keyword matching automatically detects abusive content. Suspicious messages are flagged and emphasized in the “community monitor view” user interface.

The research coordinator performs a regular *privacy breach audit* (Level 2 scrutiny). A software feature supports the audit process by displaying all non-audited privacy breaches for a given period. The coordinator investigates each privacy breach, marks it as “audited,” and provides an audit comment. The coordinator often contacts staff members via email if something is unclear. A report is printed and brought to a monthly management meeting, which discusses the current privacy breach situation. If there are privacy breaches with an unclear rationale, management initiates an investigation to identify potential misuse of information, and appropriate actions are taken. Another recurring activity in management meetings is to reflect on possible process improvements concerning privacy and accountability. Information from the above three protocols, along with queries into logged data, meeting notes, policy descriptions, and archived documents, effectively prepare the organization to respond well to *external audits* (Level 3 scrutiny) that may occur at any time.

B.4. Implementation of Breaking the Glass Principle

Three staff roles are allowed to “break the glass” in daily operations. *First*, psychologists, who may need to breach privacy (1) if there is a therapeutic emergency or (2) when the patient journal needs to be updated. *Second*, IT support staff, who need to identify a user by user id or nickname based on some personal information (name, phone number, or email). Without managing the true identity of the person, they cannot help the participant solve technical problems. When support staff breach privacy, the privacy breach rationale will automatically be set to “support,” and a reference to the support issue id will be stored. *Third*, the research coordinator can also access the support staff's view of the system in case unforeseen things happen and there is an urgent need to identify an individual participant. All three roles may access the personal identity of participants only via the software user interface after reading a warning message, and the privacy breaches are logged for auditing.

About the Authors

Jonas Sjöström. is an associate professor at Uppsala University, Sweden. He received his PhD from Uppsala University. Sjöström's work has been focused on design science research and appeared in IS journals and conferences as well as in eHealth journals, e.g., *Journal of Medical Internet Research.* Special interest has been paid to eHealth, pragmatist philosophy, and engaged scholarship, and Sjöström is the acting president of the AIS special interest group on pragmatist IS research (AIS SIGPrag).

Pär J. Ågerfalk. is a professor at Uppsala University, Sweden, where he holds the Chair in Information Systems. He received his PhD from Linköping University and has held full-time positions at Örebro University, University of Limerick, and Jönköping International Business School. Prof. Ågerfalk is a Fellow Award recipient and Distinguished Member Cum Laude of the AIS. Most recognized for his work on open-source software and agile methods, his current research centers on the orchestration of digital practices and how pragmatism and institutional theory can inform information systems development and conceptual modeling. Ågerfalk's work has appeared in several leading Information Systems journals, including *MIS Quarterly, the European Journal of Information Systems*, and *Journal of Information Technology*.

Alan R. Hevner. is a Distinguished University Professor and Eminent Scholar in the School of Information Systems and Management in the Muma College of Business at the University of South Florida. Dr. Hevner's areas of research interest include design science research, digital innovation, information systems development, software engineering, distributed database systems, and healthcare systems. Dr. Hevner received a PhD in computer science from Purdue University. He has held faculty positions at the University of Maryland and the University of Minnesota. Dr. Hevner is a Fellow of the AAAS, a Fellow of the AIS, and a Fellow of IEEE. He is a member of ACM and INFORMS. Additional honors include selection as a Parnas Fellow at Lero, the Irish software research center, a Schoeller Senior Fellow at Friedrich Alexander University in Germany, and the 2018 Distinguished Alumnus award from the Purdue University Computer Science Department. From 2006 to 2009, he served as a program manager at the US National Science Foundation (NSF) in the Computer and Information Science and Engineering (CISE) Directorate.