Exploring Privacy Attitudes and Accurate Information Disclosure in Healthcare Contexts

Autumn Clark
Virginia Tech, autumnpclark@gmail.com

Mark J. Keith
Brigham Young University, mark.keith@gmail.com

Tamara Masters
University of Utah, tamara.masters@utah.edu

Recommended Citation

Exploring Privacy Attitudes and Accurate Information Disclosure in Healthcare

Completed Research Paper

Autumn Clark
Virginia Tech University
Blacksburg, Virginia, USA
autumnpc@vt.edu

Mark J. Keith
Brigham Young University
Provo, UT, USA
mark_keith@byu.edu

Tamara Masters
University of Utah
Salt Lake City, Utah, USA
tamara.masters@eccles.utah.edu

Abstract

Patients lie to their doctors for a variety of reasons such as judgement, embarrassment, and financial concerns. These reasons are different from consumer contexts where information disclosure risks include the loss of data to unknown third parties. Yet, the same theories are commonly used to frame both settings. This overextension of theory leads to important differences in the results of these studies. We propose that additional theorizing is needed to reconceptualize privacy calculus to more accurately explain healthcare patient disclosure. Using a hybrid methodology based on both a grounded theory approach and construal level theory, this study explores the perceived risks and benefits of health data and consumer data disclosure. The results reveal significant differences in psychological distance and construal levels between the two contexts which can improve future theorizing. This deeper understanding could help improve the accuracy of patient disclosure and reduce harm in clinical systems.

Keywords: information privacy, disclosure, healthcare, construal level theory, critical realism, grounded theory

Introduction

Information privacy concerns and disclosure behaviors are unique in the healthcare setting from traditional consumer contexts (Keith et al., 2022). For example, while consumers are more concerned about issues like secondary use by third parties (Smith et al., 1996), patients are more concerned about the embarrassment and judgment from providers (Vogel, 2019). In both cases, the privacy concerns lead to either lying in the information disclosed (Jerrold, 2011; MedicareAdvantage.com, 2018) or limitations in the amount of information tracking allowed via privacy settings (Almuhimedi et al., 2015). However, the consequences of lying or withholding information are drastically different in each case. With consumer accounts and applications, withholding information may simply result in limited personalization and utility for the consumer. But for the patient, the result could be misdiagnosis (Palmieri & Stern, 2009) and potential death (Shojania & Dixon-Woods, 2017). Given that approximately 1 in 20 patients are affected by some form of preventable harm (Panagioti et al., 2019), it would be a great benefit to understand why patients disclose inaccurate information.

Despite the important differences between the healthcare and traditional consumer contexts, academic research in healthcare privacy has largely adopted the existing theories from business research such as privacy calculus (Dinev & Hart, 2006; Laufer & Wolfe, 1977) with some adaptation (e.g., Cherif et al., 2021; Dinev et al., 2016; Harborth & Pape, 2022; Keith et al., 2022; Li et al., 2016; Lustgarten et al., 2020). Privacy calculus frames information disclosure decisions as a rational tradeoff between the risks and benefits of disclosure in a particular context. Yet, there are significant differences in the risks and benefits of a healthcare setting versus consumer application context that are not fully understood that may limit the applicability of privacy calculus theory as a blanket explanation for all situations including healthcare.

For example, there are differences in the types of information collected as well as who that data might be exposed to. Traditional e- and m-commerce contexts collect data about names, emails, phone numbers, addresses, and anything else needed to personalize services and offerings whereas healthcare requires data about the body or mind. Health data is sensitive and personal to individuals and will be shared with doctors, nurses, and other providers whereas consumer data is not typically analyzed by a human, but rather, used in automated systems for machine learning unless that data is breached and collected by a hacker.

In addition, there is a great difference in the temporal immediacy of the risks of health data disclosure (e.g. immediate embarrassment and judgment from doctors of sensitive information) versus consumer data disclosure (e.g. eventual long-term spam or availability of data on the dark web). This is relevant because risks that may occur long into the future are often minimized by consumers (Acquisti & Grossklags, 2003). As a result, risks may not be accurately estimated in traditional consumer contexts compared to healthcare settings. Similarly, the *benefits* of disclosure are often immediate in consumer contexts relative to healthcare settings. For example, if you download an app to give you driving directions, then those benefits come immediately whereas if you seek healthcare for depression in the form of medication or therapy, it is less likely that you would find immediate results. In summary, the healthcare context is sufficiently unique that privacy and disclosure decisions need to be theorized differently from the consumer context from the ground up. To this end, we seek to understand how the information disclosure risks and benefits are different between the healthcare and consumer contexts.

Prior research has explored why patients lie to their providers (Jerrold, 2011; Masters et al., 2022; MedicareAdvantage.com, 2018; Palmieri & Stern, 2009; Vogel, 2019). Similarly, researchers have explained the variety of privacy risks relevant to consumers (Karwatzki et al., 2022). But our research question goes beyond understanding the information disclosure risks perceived in both contexts to a broader question of how the risks and benefits are weighed differently in the healthcare setting. This cannot be fully resolved with a positivist approach because so much is unknown about the information disclosure risks in healthcare settings. However, there are theories that can inform this issue. Therefore, the methodology of this paper most closely aligns with *critical realism* using abduction and retroduction (Mingers et al., 2013). Based on this framework, our main objectives within this paper are to (1) describe the events of interest, (2) retroduce a plausible hypothetical mechanism to explain these events (in keeping with critical realism methodology), and (3) present preliminary findings of our qualitative research thus far.

Having explained the events of interest above (i.e. information disclosure in the healthcare context), we find that construal level theory (CLT) describes a promising hypothetical mechanism that may offer some insight to frame the healthcare setting uniquely from the consumer context. Construal level refers to the degree of abstractness used to conceptualize objects and events beyond our own current, direct experience (Liberman & Trope, 2003; Trope & Liberman, 2010; Trope et al., 2007). Phenomena that are more "abstract" typically have weaker influence on our preferences and behavior than those that are more "concrete." Recent research has demonstrated that the construal level can explain how information disclosure risks and benefits vary in their importance in disclosure contexts (Butori & Miltgen, 2023). We propose that CLT is ideal for explaining the uniqueness of the healthcare disclosure context.

Therefore, to study this phenomenon, we executed a qualitative data collection to ask a variety of potential patients what they believe the risks and benefits of healthcare data disclosure would be for them in a particular medical context where certain data elements would be requested (height, weight, illegal drug use, prescription drug abuse, exercise, sexual activity, alcohol consumption, smoking status). In addition, we asked the same question of potential consumers of a particular mobile app designed to give personalized restaurant recommendations (body mass index, smoking status, alcohol consumption, soda consumption,

dessert consumption, fast food consumption, amount of overeating, use of diet-related medication, exercise). The data from this collection were open-ended text responses. The results were categorized using a grounded-theory approach and then juxtaposed against the various types of psychological distances (near versus far) proposed by construal theory. This combination of methodological approaches is typical of critical realism which is ideal for research contexts where neither a fully positivist or constructivist approach is completely ideal.

While the results do confirm many of the findings from prior research on why patients lie to their doctors, they also reveal new topics that were not reported in prior research. Importantly, the results also suggest that there are significant differences in the psychological distance of the risks and benefits to disclosed health data versus data needed for a consumer app—even though several of the data elements were the same in each context. The implication of this finding is that existing theory intended to explain information disclosure should measure and consider psychological distance in the risk/benefit tradeoff. Disentangling differences in risk and benefit in the commercial vs healthcare setting may enlighten how to increase the willingness to share personal information and the accuracy of information shared. This has theoretical as well as practical significance.

Patient versus Consumer Disclosure

In 2018, a US-based national survey found that as many as 81 percent of respondents have withheld medically relevant information from their clinician (Levy et al., 2018; MedicareAdvantage.com, 2018). The types of information respondents admitted to withholding from health care providers included items such as disagreement with a provider's advice, suboptimal exercise and diet habits, nonadherence to a prescription medication regimen, substance abuse, and whether they understood their provider's treatment instructions (MedicareAdvantage.com, 2018; Vogel, 2019). The most common reasons patients gave for withholding medical information from a clinician were (1) not wanting to be judged or lectured, (2) not wanting to hear how harmful their behavior was, and (3) embarrassment (Levy et al., 2018; Vogel, 2019). All the information a clinician requests from a patient during an exam has clinical significance, and attempting to treat a patient without accurate information can lead to medical errors, such as misdiagnoses or prescribing contraindicated medication (Jerrold, 2011).

Compare this with disclosure behavior in a consumer context, in which the most commonly cited reasons for withholding or misrepresenting personal information revolve around physical threats to safety, social influence, loss of money, and fear of prosecution or job loss (Karwatzki et al., 2022). We expect some level of overlap between these risks and those for the healthcare domain. However, we also expect to find a different emphasis or level of risk (i.e. the probability and impact of those risks) between those that overlap.

While the risks identified by Karwatzki et al. (2022) are legitimate and powerful predictors of consumer disclosure behaviors, they are inspired by end scenarios that are perhaps less visceral and immediate than the disapproving look or disparaging comment a patient may receive from their physician upon disclosing sensitive and embarrassing behavior. Additionally, the requested information itself in a healthcare context is often more sensitive, intimate, and/or personal than the information typically requested in a consumer context. While the mishandling of personal data commonly associated with retail transactions, such as credit card numbers or email addresses, remains a source of distress and concern, the potential repercussions are generally less intimate and consequential compared to the mishandling of health data. This is because retail-related details primarily pertain to transactional aspects and do not offer profound insights into an individual's personal identity, lifestyle, or well-being, as is often the case with health information.

Despite these differences in the perceived risks of disclosing accurate information between consumer and patient contexts, privacy calculus theory is perhaps the most used framework for both settings (Cherif et al., 2021; Dinev et al., 2016; Harborth & Pape, 2022; Li et al., 2016; Lustgarten et al., 2020). While privacy calculus has proven effective in explaining a significant degree of consumer behavior, it has limitations centered around its assumption of humans as rational actors who can adequately estimate and quantify the risks and benefits of disclosure. However, as indicated above, there may be significant differences between the consumer and patient context in our ability to assess perceived risks and benefits. Next, we theorize one way to differentiate these two contexts.

Construal-Level Theory and Psychological Distance

Construal-level theory (Trope & Liberman, 2010; Trope et al., 2007) provides a framework that is particularly well-suited to highlight the differences between the risk and benefit perceptions that determine information disclosure in the healthcare context versus traditional consumer electronic accounts. Construal level indicates how abstractly (high level construal) or concretely (low level construal) information is processed. A concrete mindset refers to thinking about the how of a task. For example, rubbing a toothbrush across your teeth is low-construal or a concrete aspect of tooth-brushing, while abstract (high level construal) aspects of toothbrushing would be to prevent tooth decay. In a concrete mindset (i.e., low-level mental construal), the value of a product is not abstract or emotional but rather cognitive in terms of likelihood of outcomes (Hong & Lee, 2010). Low construal thinking individuals focus on the details of the task (Mehta et al., 2014).

The level of concreteness at which an individual constructs a situation can be affected by situational factors (Vallacher & Wegner, 1987; Wegner & Vallacher, 1986). For example, low construal thinking can be triggered by asking individuals how to accomplish a goal (Fujita et al., 2006), by thinking of more proximal events (Liberman & Trope, 2003), and by providing higher goal specificity and importance (Ülkümen & Cheema, 2011). For example, low construal would be how to provide answers to get a prescription to heal a sore throat, versus high construal of what to do to get a visit with a physician to get better. Trope and Liberman (2010) propose two criteria for determining which features of an object are high level and which are low level: centrality and subordination. High-level features play a more central role in the meaning of an object; therefore, altering a high-level feature will have a greater impact on the object's meaning compared to modifying a low-level feature. Additionally, low-level features derive meaning from high-level features to a greater extent than the reverse. In the example of attending a lecture, the topic of the lecture is both more central than and superordinate to the location of the lecture, and the topic thus constitutes a higher level of construal than location.

The level of construal concreteness (low construal) or abstractness (high construal) is tightly related to and commonly approximated using psychological distance. In construal theory, four types of psychological distance are identified: temporal, spatial, social, and hypothetical. Temporal distance refers to the timing of events: whether they will occur sooner (low construal) or later (high construal). Events that are expected to occur further in the future are harder to conceptualize. This temporal distance leads decision makers to discount future events and devalue positive future outcomes (known as hyperbolic discounting) (Acquisti & Grossklags, 2003; Laibson, 1997). Spatial distance is the physical proximity of events. For example, sharing data with a doctor that is going to be seen face-to-face in the next room is a low (concrete) construal compared to high construal (abstract) of losing data to a third party overseas who you will never meet personally. This example also applies to social distance which refers to the relationship space between people or groups. A patient may develop a relatively close personal relationship with a doctor over time. Even seeing the doctor face-to-face once without ever seeing them again represents a much lower and more concrete construal level than an unknown hacker who steals your data who you will never meet personally. Finally, hypothetical distance refers to the likelihood that an event will occur. A likely event is low-construal, concrete, or "near" versus an unlikely event that is high-construal, abstract or "far". For example, a patient may believe that it is very likely that they will get into legal trouble for sharing their illegal drug use versus unlikely that they will suffer from identify theft from having their password stolen.

There is a small but growing body of research that utilizes CLT to examine privacy behavior (Bandara et al., 2018; Cloarec et al., 2022; Hallam & Zanella, 2017; Singh et al., 2018). However, two are particularly relevant to our context. First, only one addresses the healthcare context (Singh et al., 2018) but applies specifically to healthcare data breaches which is an important, but distinct, topic from ours. Second, and most relevant to our context, Butori and Miltgen (2023) use construal level as a moderator of perceived risks and benefits. They found that only concrete (as opposed to abstract) risks caused consumers to reduce their information disclosure.

This is meaningful to our purpose if the types of data and risks associated with that data in the healthcare context have greater "concreteness" than traditional consumer contexts. If true, then this would explain differences in the strength effect sizes of perceived risks versus benefits in the privacy calculus that consumers/patients formulate to make disclosure decisions. Figure 1 visualizes the implications of our

propositions for privacy calculus theory which would account for the healthcare and consumer contexts by incorporating construal level and psychological distance.

Figure 1. Construal-Based Privacy Calculus Model for Future Research
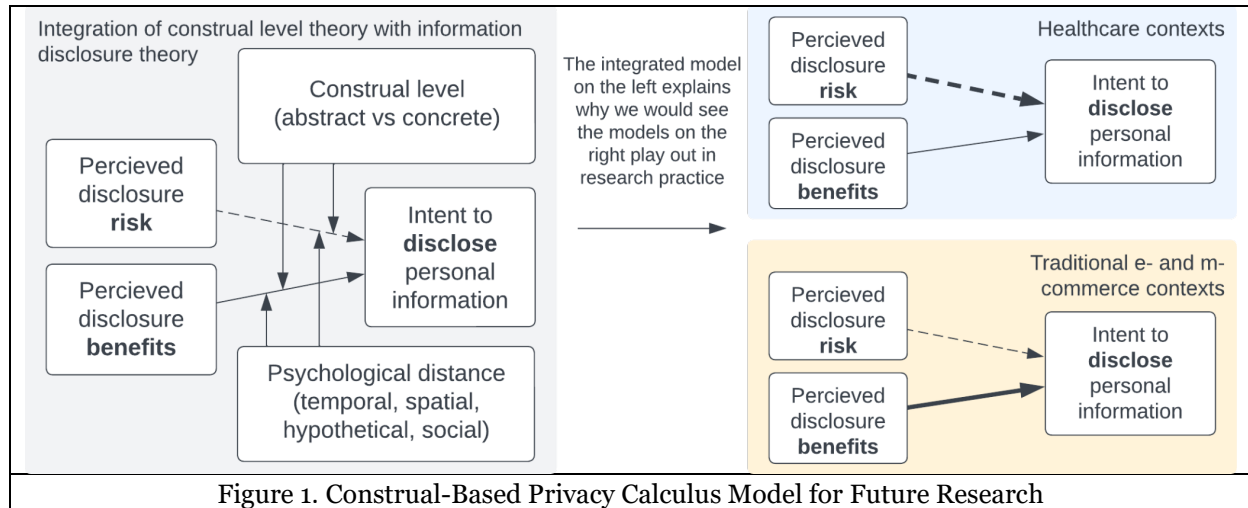
Essentially, construal level and psychological distance moderate the effect of perceived risks and benefits on information disclosure depending on the context. In healthcare, we expect that the risks identified in prior literature like embarrassment, judgement, and financial or job loss are more concrete and psychologically near to individuals. Thus, perceived risks will have a larger (negative) effect on reducing information disclosure than perceived benefits have on increasing disclosure leading to a greater amount of lying to healthcare providers. In more traditionally studied e- and m-commerce contexts, the benefits of disclosure (e.g. personalized recommendations) are easier to construe and psychologically close to consumers; thus, leading to perceived benefits having a larger effect on disclosure (e.g., Keith et al., 2015; Keith et al., 2013).

However, although we have stated some expectations about the differences in the concreteness of perceptions between the risks and benefits of health data versus consumer data, we do not feel it is appropriate to hypothesize these differences without first better understanding the actual risks and benefits associated with each context. This is because psychological distance is typically measured in specific contexts as opposed to general categories like perceived risks and benefits are often measured. For example, we could not ask a research participant to tell us how concrete or abstract the risks and benefits of health data are without referring to specific data elements (e.g. name, address, phone number, height, weight, exercise, alcohol consumption, depression, anxiety, etc.).

Therefore, the purpose of this research (as stated earlier) is to identify a list of perceived risks and benefits associated with health data versus consumer data elements so that we can categorize those risks and benefits and differentiate them by construal level's psychological distance.

Methodology

Critical realism asserts an ontological distinction between the real world and our knowledge of it (Bhaskar, 2013). It contends that there are real, underlying mechanisms (in this study, construal level) that might produce observable events, even if the mechanisms themselves are not always observable. This philosophy guides our exploration of how construal level may influence perceived risks and benefits of disclosure in various contexts, and we felt this was an especially relevant approach, given the difficulty of observing and empirically quantifying the process by which individuals make disclosure decisions. By acknowledging the real-world implications of disclosing health data and understanding that our perceptions of these risks and benefits can vary, we employ a research approach that is both realistic and sensitive to our subjective interpretations.

Although we have some expectations regarding construal level and psychological distance, we must use an interpretive, grounded theory approach to understand how the specific types of perceived risks and benefits

are different in health data. Grounded theory has been often used in both healthcare research (Cutcliffe, 2000; Walker & Myrick, 2006) and information systems research (Urquhart et al., 2010; Wiesche et al., 2017). Grounded theory uses inductive reasoning based on qualitative data where ideas and concepts emerge from data (Glaser & Strauss, 2017). Specifically, it calls for an initial coding of distinct ideas or themes in the data, achieved by continuously comparing each new data point with the existing codes to determine fit, followed by an examination of the relationships between these categories (referred to as axial coding). Grounded theory is appropriate in our context because, as mentioned above, prior research on the risks and benefits of information disclosure are largely based in the context of e- and m-commerce which may not be sufficient to hypothesize about concepts like construal level and psychological distance. In line with the principles of critical realism, we recognize that our interpretations emerge from real-life experiences, but these interpretations are socially and culturally mediated. If we are to understand specific risk and benefit perceptions regarding health data, we must start with a qualitative data collection.

To collect data for our study, we created vignettes for two hypothetical, but specific, information disclosure contexts that could be relevant to people from a wide range of backgrounds. Participants were randomly assigned to the health care or consumer mobile app disclosure survey. The health care survey began by explaining to participants that we were mental health researchers who wanted to understand the causes of depression in adults. We chose depression research as our premise both because of its relevance, as an estimated 30 percent of adults in the US report being diagnosed with depression at some point in their life (Witters, 2023), as well as to enhance the believability of our survey, as depression is a widely-recognized health condition with standardized measures that could feasibly be screened for online. Participants were informed:

> *We are working to better understand the causes of depression in adults. To do so, we need to clinically measure and assess depression in individuals and ask them for important health background data including: height, weight, smoking, tobacco & vaping usage, alcohol use, illegal drug use, prescription drug misuse, sexual activity, and exercise regularity.*

> *While disclosing each of these health data points accurately and honestly may help providers better diagnose and treat symptoms of depression, it also comes with certain risks that may cause patients to lie or exaggerate their responses. We ask for your help in coming up with a list of all potential risks and benefits of sharing this data. Please think carefully about what you personally would be concerned about when sharing this data and what benefits you would hope to receive from sharing this data.*

The second context was a consumer mobile application. For this, our goal was not to select a context that would represent all possible range of contexts. Rather, our purpose was to learn how the psychological distance differed between risks and benefits in a sample consumer context that might be somewhat comparable to the healthcare context chosen. Therefore, we selected the context of a restaurant recommender app because it could require certain data fields similar to the health context. The participants were told:

> *We are working to develop a better algorithm for a mobile app that recommends restaurants. To do so, we need to assess food preferences in individuals and ask them for important background data including: BMI, smoking, alcohol consumption, carbonated beverage (soda) consumption, dessert consumption, fast food consumption, overeating, use of diet-related medication, and exercise.*

> *Although having this data will help us give customers a more accurate restaurant recommendation, it is possible that customers will be hesitant about the risks of sharing personal information. We ask for your help in coming up with a list of all potential risks and benefits of sharing this data. Please think carefully about what you personally would be concerned about when sharing this data and what benefits you would hope to receive from sharing this data.*

To preserve the believability of the premise of the survey, we needed to find related or substitute measures for some data fields (e.g., it would be suspicious for a restaurant recommender app to require users to disclose their height and weight, but BMI is a related, comparably sensitive measure). We were unable to identify a non-healthcare commercial context in which the exact questions used in a medical screening

survey could be posed without arousing suspicion and jeopardizing the results of the study. Indeed, the premise of this study is that the data required, and risks involved in each setting are very different. We thus concluded that using questions appropriate in a near approximation (such as a restaurant recommendation context) represented a weaker threat to the validity of our results. Although the data elements being collected in each context are not perfectly aligned, the restaurant recommender context allows us to base the differences in responses more on who the data are being shared with as opposed to what data is being shared—at least relative to other consumer contexts. After reading the text, participants were given a list of textboxes to enter their responses into and were required to enter at least two risks and two benefits with the option of entering up to ten for each. Participants were randomly assigned to respond to only one of the health or consumer contexts, but not both.

We received a total of 684 responses between two surveys and we implemented a survey design that ensured participants' responses were limited to a single context. Approximately two-thirds of these responses were collected from Prolific and the other third from MTurk which have been demonstrated to provide results at least as valid as those of a professional online panel (Lowry et al., 2016; Palan et al., 2018). Two-hundred and eighty-two responses were dropped either because they missed a trap question or provided no relevant text responses to be analyzed. Of the remaining 402 responses, 202 completed the procedures for the mental health context and 200 for the mobile app context. Of those who chose to report, this sample was represented by 51.6 percent females, 70.6 percent Caucasians, 5.5 percent African Americans, 5.2 percent Asians, 5.0 percent mixed ethnicities, 4.0 percent Hispanics, 3.0 percent other, and 1.5 percent Native Americans. The average age was 35.8 years old. Online panels were utilized to more accurately reflect the method of providing private information online and to increase the diversity of our sample population beyond what a local focus group could provide.
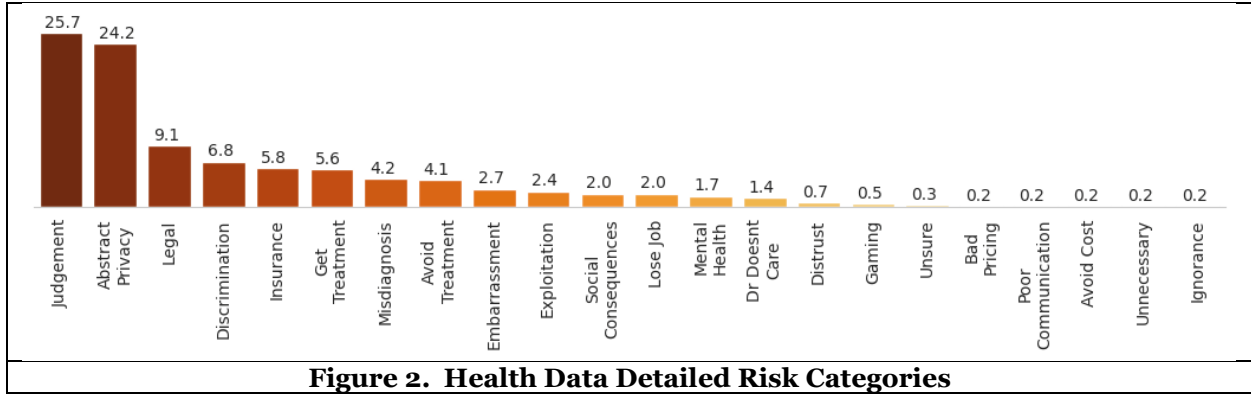
Our coding process was conducted by three researchers. The initial open coding and comparison process for each pool of responses (health data risks, consumer data benefits, etc.) was carried out by a single researcher, to promote familiarity with the data and category coherence. Categories were intended to be mutually distinct; multiple benefits or risks could be identified in a single participant comment, and coding processes reflected this. Because of the manageable number of responses collected, open coding was carried out for all responses, rather than coding until saturation was perceived. Axial coding and any ambiguous cases were then discussed by the three researchers until a consensus was reached, with an emphasis on identifying themes in the risks and benefits that applied in both contexts and spanned both concrete and abstract outcomes. For the risks, we then mapped the categories to the dimension identified by Karwatzki et al. (2022). Given the absence of an established framework for potential disclosure benefits, the higher-order categories were systematically formulated by our research team. This process was in line with critical realism's emphasis on epistemic relativism, acknowledging that while we're aiming to understand real-world phenomena, our categorizations are influenced by our historical and cultural standpoints.

Results

Health Data Risks

Figure 2 visualizes the percentage of the detailed categories coded about each identified health data risk. Like prior health care disclosure research, the primary concern was the fear of judgment and embarrassment (25.7 percent). The next most common risk was abstract, non-specific privacy (24.2). Although every issue could be considered a "privacy" concern in the broadest context, this category covers remarks that were either non-specific privacy risk or secondary use by third parties. This type of concern (which often showed up in the written participant remarks as simply the term "privacy") does not fit in the specific categories outlined by Karwatzki et al. (2022). Legal concerns (9.1 percent) were the next most common which may be the result of including illegal drug usage as one of the data points in question.

The fear of discrimination (6.8 percent) by the hospital and doctors themselves was the next most common concern. The risk of insurance costs rising (5.8 percent) was next, followed by the fear of mistreatment which included not only misdiagnoses (4.2 percent), but both a desire to get the treatment they *did* want (5.6 percent) and avoid the treatment they *didn't* want (4.1 percent). Embarrassment (2.7 percent) came next followed by exploitation or blackmail by others (2.4 percent). Social consequences (2.0 percent) included the worry that spouses, children, or other loved ones would find out about bad behaviors.

Figure 2. Health Data Detailed Risk Categories

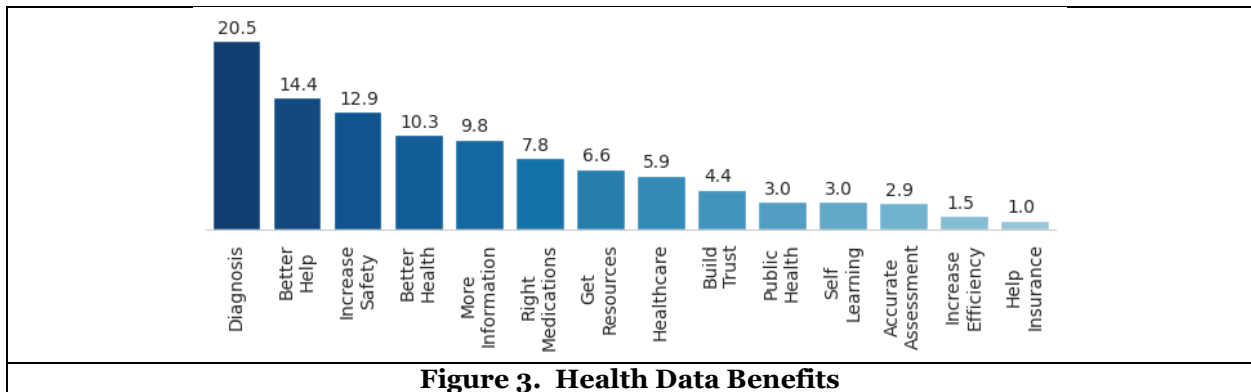| High Level	Category	Example Statements
Social	Judgment	"I don't want the doctor to judge me."
	Embarrassment	"It's just generally embarrassing for people to know how much you drink or that you never exercise."
	Discrimination	"The doctor might discriminate against me because I'm overweight."
	Exploitation	"Knowing a person's sexuality can be negative when that information is used without consent and to do harm against LGBTQ people."
	Relationship	"I don't want my kids to know my lifestyle." "My partner might find out about my sexual activity."
	Distrust*	"Doctor might not take you as seriously if you did not disclose before, but now you do. Trust issues moving forward."
Psychological	Mental health	"It might affect my mental health to talk about weight." "All of the questions in general just make me anxious."
	Dr doesn't care*	"Healthcare providers don't take patient's problems seriously, it's just another case for them."
Abstract privacy*	Non-specific privacy*	"My data could be lost or stolen and shared with third parties."
Prosecution-related	Legal	"Disclosing your illegal drug use could result in jail time."
Resource-related	Insurance	"Insurance companies might charge me more if they knew how unhealthy I am."
	Avoid cost	"The doctor may find something expensive wrong with me."
	Bad pricing	"They may offer different pricing based on the data I give them."
Treatment*	Misdiagnosis*	"Healthcare provider may dismiss other symptoms due to being overweight or not active enough."
	Get treatment*	"Revealing past drug misuse may lead the provider to blacklist many viable options for medication for you."
	Avoid treatment*	"If you are honest some might be afraid of being committed to a mental health institution."
	Gaming*	"Doctors assume patients are lying about the amount they smoke or drink and add on to the number given, so giving an honest number means the doctor will calculate it high."
	Unnecessary*	"Patients might not be given an explanation for needing this information and feel it is unnecessary."
	Unsure*	"I may not remember the information exactly so it's better not to share it."
	Ignorance*	"I'd rather not know just how unhealthy I am."
	Poor communication*	"Language barriers might make someone hesitant to share data because they worry they can't fully explain themselves"
Career-related	Lose job	"If my work finds out about my drug use, I'll lose my job."

Table 1. Health Data Risk Categories and Examples

While the concerns above were most common, there were some less frequent, but very interesting concerns that have not come up in prior research that were primarily related to uncertainty. For example, there was a concern that one's mental health would suffer from sharing sensitive information as well as a belief that doctors do not care so they don't need to know. Also, one self-admitted doctor said that they always assume that patients lie and exaggerate how little they drink alcohol or use drugs, and patients know that doctors assume that. Therefore, the patients will admit only half of their actual drug use, for example, knowing that the doctor will assume an amount double that size. This is a form of "gamified" lying. Distrust refers to when a patient has lied in the past so they must lie again or else the doctor will no longer trust them. Other minor issues included not being sure if the patient remembers their information correctly, not knowing why the data is needed, or simply preferring not to know just how unhealthy they might be.

In Table 1, we map the detailed categories found during coding to the higher-level categories identified by Karwatzki et al. (2022). We placed asterisks next to categories that were not explicitly included in that prior research. In addition, we provide example statements from respondents to represent each category. The primary difference in our findings was the concern about *treatment* which we believe is distinct from the *physical* privacy risk category identified by Karwatzki et al. (2022). In their study, physical risk referred to issues like physical assault whereas treatment refers to the concern that disclosed information may result in a misdiagnosis or the inability to get or avoid treatments. Treatment risks are much more concrete and psychologically "near" from a CTL perspective than the chance that someone might come to your home and assault you.

Health Data Benefits

The results of the health data benefits categorization are found below in Figure 3 and Table 2. Because Karwatzki et al. (2022) did not develop a framework around disclosure benefits, we include our own higher-level categorizations. Similar to the healthcare risks, participants were able to produce a wide range of benefits indicating that they are also more concrete and easier to construe or more psychologically "near." The primary benefit perceived was an accurate diagnosis (20.5 percent). However, a variety of other interesting benefits arose we well including better overall help from the provider (14.4 percent), greater patient safety (12.9 percent), better long-term health (10.3), more information (9.8 percent), more appropriate medications (7.8 percent), access to resources (6.6 percent), and more.

Figure 3. Health Data Benefits

High Level	Category	Example Statements
Overall health	Better health	"better more informed care plan"; "foundation to begin treating you"; "allows one to see behavior that is not healthy"; "get better health"
	Diagnosis	"a clearer picture of what is wrong with you"; "deeper understanding of the cause"; "accurate diagnosis"
	Right medications	"better prescription"; "prevent medication errors"'
	Get resources to help	"better recommendation for treatment"; "provide additional services for things like substance abuse";
	Get better help	"better education from Dr"; "make most informed decisions"; "better help"; "provide better referrals"
	Increased patient safety	"avoid medication errors"; "know risk factors can influence treatment methods"
	Accurate risk assessment	"this data could help the provider be aware of potential conditions that might crop up for the patient"; "an accurate risk assessment"
Knowledge-related	Provide more information	"better information for studies"; "administrative"; "medical records"; "consistent overall view of trends"; "research acceleration"
	Self-learning	"can know about your body"; "you can understand how you are coping"; "the patient would have to confront the truth about their habits"
Social	Build trust	"potential for human connection/kindness"
Resource-related	Help insurance	"insurance premium might be lowered"; "save the customer money"; "potentially lower insurance rates"
	Increase efficiency	"more efficient healthcare"; "reduce wait time"; "save time"; "reduce unnecessary testing"
Table 2. Health Data Benefits Examples		

Consumer Data Risks

Figure 4 and Table 3 illustrate the frequency of consumer data risk categories. Abstract, non-specific privacy concerns were the most prevalent by far (49.4 percent), almost outnumbering the other 15 categories combined indicating the difficulty that respondents had in conceptualizing consumer data risks. All remaining categories matched to the higher level categories identified by (Karwatzki et al., 2022). The second most cited risk was receiving targeted advertising (8.5) due to shared information. The third most common concern was experiencing negative feelings like shame or anxiety (8.0 percent) from sharing information. This was distinct from the fear of judgment by others (6.3 percent), as negative feelings were tied to the act of disclosure, regardless of whether someone else saw the information.

Users also expressed concerns about the recommender app's interface and algorithm, including its potential simplicity leading to inaccurate recommendations or the promotion of unhealthy food despite users' intentions. Conversely, users worried about the app forcing healthy options and limiting their agency. Although these concerns were generally considered benign, bias (discrimination) and exploitation were more sinister. Algorithmic bias and discriminatory treatment from partner restaurants were concerns, as well as the app deliberately recommending unhealthy options or selling information to third-party advertisers for exploitation. Other common concerns included the necessity of requested information, financial implications like insurance rate adjustments, and potential legal, professional, and social consequences. However, these concerns were cited less frequently than in a healthcare context.
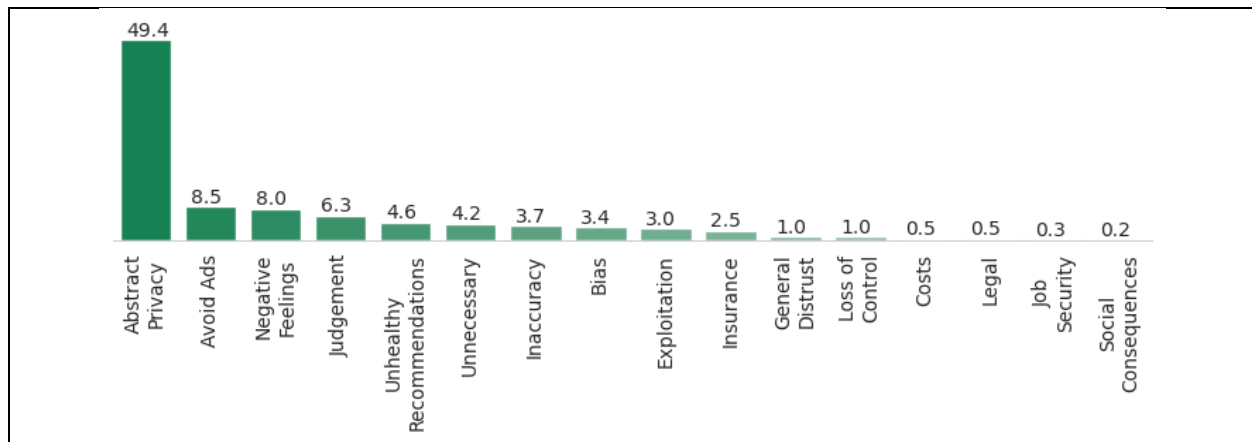
Figure 4. **Consumer Data Risks**

High Level	Category	Example Statements
Abstract Privacy*	General Privacy	"They now have this info and can do whatever with it"; "privacy"
	Unnecessary	"It seems like an invasion of privacy and unnecessary to ask about exercise, medication, fast food and soda consumption, dessert, smoking and BMI. I wouldn't share this in any app."
Psychological	Negative Feelings	"Inputting this information could make users feel embarrassed or self-conscious"; "There is no risk in the app itself, but I would worry about this data being sold to other companies and that I may be profiled as a smoker"
	General Distrust	"Not understanding what the data is used for, a fear of the unknown for the average consumer"
Freedom-related	Inaccuracy	"The data collected could also be used to make inaccurate or biased recommendations. For example, if the app was to use the data to recommend restaurants based on BMI or activity level, then this could lead to recommendations that are not reflective of user preferences."
	Loss of Control	"The app might take personal choice away from the person by deciding they need to eat healthier."
Resource-related	Avoid Ads	"There is no risk in the app itself, but I would worry about this data being sold to other companies and that I may be profiled as a smoker"
	Exploitation	"Data could be used to take advantage of my vices/cravings"
	Insurance	"If sold, could it impact my insurance rates (I.e., my health statistics may raise my health insurance rates due to higher likelihood of illness)"
	Costs	"Potential for discrimination or extra charges from restaurants should they obtain this data in some way. E.G. being charged more on basis of one's BMI."
Social	Judgment	"I'd be vulnerable to fat shaming, intrusive diet recommendations, or unwelcome comments"
	Discrimination	"I'd receive biased recommendations based on perceptions of weight and activity"
	Social Consequences	"A partner could view your data or preferences and find out something they didn't know about you"
Physical	Unhealthy Recommendations	"The app using my bad eating habits against me (recommending unhealthy food that I have a habit of eating)"
Prosecution-related	Legal	"Exposing underage drinking"
Career-related	Job Security	"Your employer could somehow get this data and fire you for something they didn't like"
Table 3. Consumer Data Risks Examples		

Consumer App Data Benefits

The results of the consumer data benefits categorization are found below in Figure 5 and Table 4. Participants identified the algorithm's ability to offer personalized recommendations as the primary benefit of disclosing the requested information (46.4 percent), next noting that disclosure might allow for recommendations that were more health-conscious, adapted to a user's dietary preferences or restrictions, or better suited to an individual's unique palette. The second most cited category identified the app's ability to provide the user with information and insights both about the offerings at various restaurants along with their own physiological and behavioral data. Following this, the next benefit users cited was the ways the app would make the selection of restaurants easier, such as the convenience afforded by outsourcing the decision and the possibility of receiving recommendations for a wide variety of restaurants.
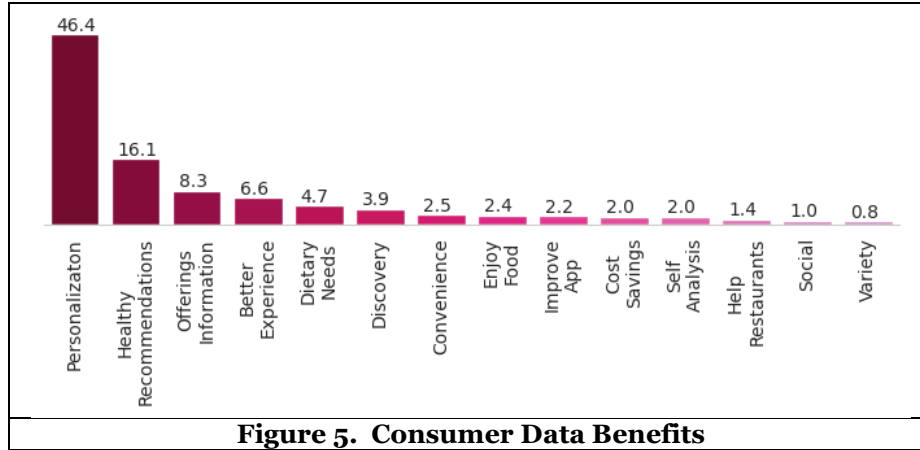

Figure 5. Consumer Data Benefits

High Level	Category	Example Statements
Appropriate Recommendation	Personalization	"Customized recommendations so there's less chance of a bad match."
	Healthy Recommendation	"Could recommend healthier options similar to a person's unhealthy eating habits"
	Dietary Needs	"Can help those with food allergies avoid places that will trigger the allergies"
	Enjoy Food	"Dishes or drinks that may interest you"
	Discovery	"The app could help you discover a restaurant you would not have tried previously."
	Convenience	"Not having to manually search for a restaurant that caters to my needs"
	Variety	"Get to try new places or different places"
Knowledge-related	Offerings Info	"No accidentally dining at a place that doesn't serve alcohol when you wanted a drink and vice versa"
	Self-Analysis	"The data can be used to help users monitor their eating habits."
	Improve App	"gain better insight so that app works better"
	Help Restaurants	"Could help restaurants come up with new menus or dishes to meet trends in user interest"
Social	Better Experience	"Depending on how it's asked, people may feel seen but without judgment, therefore going to the recommended restaurants and potentially having a better, more supportive experience."
	Social	"recommend you places with patrons of similar lifestyle"
Resource-related	Cost Savings	"give offers for deals related to preferences"
Table 4. Consumer Data Benefits Examples		

A smaller but notable proportion of participants listed benefits that did not directly affect themselves, such as improving the algorithm and app by providing additional data, as well as helping local restaurants by

potentially driving more traffic to them and helping them better cater to the dietary preferences in their area. These comments can be seen as more distant from the self and thus a higher more abstract construal-level. A few participants also identified an improved dining experience (such as finding restaurants with smoking areas or connecting with similar people at a restaurant) and financial savings (such as receiving recommendations for restaurants with specials or discounts) as possible benefits motivating disclosure. These comments can be seen as closer to the self, or the how of experience and lower more concrete construal-level.

Discussion

The purpose of this study was to demonstrate how the risks and benefits of healthcare data disclosure differ from consumer contexts in their construal level and psychological distance. In addition, we set out to identify those specific risks and benefits so they can be measured properly in future research. By positioning our findings within an existing framework of consumer privacy risks (Karwatzki et al., 2022), we have been able to identify some uniqueness.

For example, one interesting finding from the data above is the number of health (n=22) versus consumer data risks (n=16). It seemed easier for participants to come up with a variety of risks for health data that were more evenly spread across many topics compared to consumer data which were almost primarily abstract privacy risks which were not easily tied to the more specific risks outlined by Karwatzki et al. (2022). This speaks to the construal level in terms of psychological distance of the two data types. Participants have more concrete (lower) risk concerns with health data than consumer data. In particular, abstract privacy risk came up 292 (49.4 percent) times with consumer data and only 143 (24.2 percent) times with health data where it was also only the 2nd most common topic as opposed to the overwhelmingly topmost common topic with consumer data.

In addition, the healthcare context has unique risks and benefits have different levels of construal and psychological distance from consumer contexts. Most significantly, our respondents identified risks associated with getting treatment for their health issues. Some wanted to avoid painful treatment while others wanted to get the right treatment. Some were worried that miscommunication or language barriers would result in incorrect treatment. Others tried to "game" their treatment by anticipating that the doctor would assume they were understating their poor health behaviors. These risks are more concrete and easier to conceptualize than most consumer risks which are difficult to predict. They also have nearer psychological distances because mistreatment will happen immediately and can be more directly tied to a specific information (non)disclosure.

Another example is that the fear of social consequences like judgment and embarrassment is much stronger with health data. This risk is both spatially and socially close, low construal, or "concrete" because it will happen face-to-face with a person that the patient may have to see repeatedly. Although your doctor may not be family or your best friend, they are a relationship that is much closer than an unknown hacker overseas. Similarly, the likelihood and timing of that embarrassment is also very close compared to some eventual data breach by an unknown hacker that could happen sometime in the future.

The psychological distance of health data disclosure risks is also much closer and more concrete relative to the benefits. The primary benefits are a more accurate diagnosis and better help, treatment, and health which is based on the self. However, a patient is not as sure that a treatment will work as they are that they will be embarrassed when sharing health data. Similarly, it takes time for surgeries, medications, and other changes to take effect compared to the judgment that may happen immediately when the doctor reads your file and enters the room. Table 5 summarizes the differences in psychological distance for health data risks versus benefits which forms the reasoning for Proposition 1.

	Spatial	Social	Hypothetical	Temporal
Health data risks	Close (low)	Near (low)	Likely (low)	Immediate (low)
Health data benefits	Distant (high)	Far (high)	Unlikely (high)	Long-term (high)
Table 5. Summary of Psychological Distances across Healthcare Data Types				

Proposition 1: The perceived risks of health data disclosure have lower (a) social, (b) hypothetical, and (c) temporal distance than the perceived benefits.

The implication of P1 is that information disclosure decision models will be affected more by perceived health data risks than benefits. The greater psychological distance of perceived benefits means that phenomena like hyperbolic discounting will play a larger role when assessing perceived benefits because the benefits will occur further into the future than the risks. This can explain why patients are well-known for lying to their providers when required to fill out intake forms.

With consumer data, the risks are much more psychologically distant than the benefits. For example, the benefit of using a recommender app is that the consumer will get a personalized recommendation immediately that is more temporally close than a data breach that could happen sometime in the future. The recommendation is also much more likely to happen, and the benefits will be shared with people that are spatially and socially closer to you than an unknown hacker who is miles away. Table 6 summarizes these differences forming the reasoning for Proposition 2. Propositions 3 and 4 are based on both tables.

	Spatial	Social	Hypothetical	Temporal
Consumer data risks	Distant (high)	Far (high)	Unlikely (high)	Long-term (high)
Consumer data benefits	Close (low)	Near (low)	Likely (low)	Immediate (low)
Table 6. Summary of Psychological Distances across Consumer Data Types				

Proposition 2: *The perceived risks of consumer data disclosure have higher (a) spatial, (b) social, (c) hypothetical, and (d) temporal distance than the perceived benefits.*

Proposition 3: *The perceived risks of health data disclosure have lower (a) spatial, (b) social, (c) hypothetical, and (d) temporal distance than the perceived risks of consumer data disclosure.*

Proposition 4: *The perceived benefits of health data disclosure have higher (a) spatial, (b) social, (c) hypothetical, and (d) temporal distance than the perceived benefits of consumer data disclosure.*

In summary, P2-4 explain why so many studies of consumer privacy calculus find that perceived disclosure benefits are a stronger explanation of actual disclosure behavior than perceived risks (Keith et al, 2013; 2015). The benefits of e- and m-commerce applications are perceived as more likely, immediate, close, and personally near than the risks.

There are several implications of these propositions. First, if rational choice-based theories such as privacy calculus are to adequately account for a wide range of contexts including healthcare, they should incorporate construal level and psychological distance in their equations like how recent research has model CLT in the consumer context (Butori & Miltgen, 2023). This important moderator may account for the differing importance of perceived benefits and risks across contexts and provide greater explanatory power for actual information disclosure.

Next, and perhaps most importantly, to aid healthcare providers in creating accurate diagnoses and save lives, patients need to help in lowering the construal level of the benefits of disclosing accurate information. They need to know how likely it will be that they will receive the benefits of health data disclosure that they are hoping for. They need to know when those benefits to themselves will come and understand how it may impact others near to them in addition to themselves. Providers may be understandably hesitant to provide this type of information since it is impossible to promise future health. However, rational actors prefer certainty to uncertainty. Therefore, it is better to provide them with more concrete ideas to help them make better decisions with their health behavior and information disclosure.

This research reveals that context matters with differences found between commercial and health care privacy risks and benefits. With health care using many online devices and the importance of patient truthfulness on correct diagnosis and optimal care, the effect of construal should be further studied. Interviews and scale analysis for benefit categories should be done to further define the contextual impact. Further research to define construal level for all categories can be studied to determine the impact of consumer concern for privacy.

Future Research and Limitations

We employed a critical realist approach in our research. Within this paper, we executed the first two steps of critical realist methodology: (1) describing the events of interest and (2) retroducing an explanatory mechanism (construal level). The additional steps of (3) eliminating false hypotheses and ultimately (4) identifying the correct mechanism will fall to later work. We encourage other researchers to continue testing the validity of construal level as an explanatory mechanism, as well as explore the potential of other mechanisms in explaining disclosure behavior in healthcare and consumer contexts.

Although our sample included potential patients and consumers from a variety of backgrounds, Prolific and MTurk do not perfectly represent the entire population of interest. There may be risks and benefits to consider that did not come up in our dataset and risks and benefits may overlap in subtle ways. This is something that can be teased out in future research. Perhaps the primary limitation of this research is that we stopped short of creating measures of psychological distance for each risk and benefit that was raised. However, that is a clear next step for future research—to validate the assumed distances in Tables 5 and 6 by generating measures for each data type and psychological distance. Doing so would allow testing these propositions above using hypotheses. Those measures could be used to augment theories explaining information disclosure in various contexts so that health data disclosure can be more accurately explained. For example, it could explain why the perceived risks of disclosure are often a much weaker explanation of actual disclosure behavior than the perceived benefits in consumer context (e.g., Keith et al., 2015; Keith et al., 2013) whereas the opposite is true in healthcare contexts (e.g., Keith et al., 2022).

Another potential limitation of our methodology was requiring participants to provide at least two examples of risks and benefits each. We could have required more examples (up to 10 were allowed). However, doing so may have artificially inflated the occurrence of less common risks and benefits. This would have made the study less generalizable given that prior research has shown that people tend to process privacy risks in a secondary route (Lowry et al., 2012) using shortcuts and heuristics without giving deep thought to all of the risks involved.

We hope this research will be used to augment future theorizing and testing of information disclosure decisions across a variety of contexts. We also hope it will provide direction for clinicians who want to improve their patient information disclosure accuracy and subsequent diagnoses.

References

Acquisti, A., & Grossklags, J. (2003). *Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior* UC Berkeley 2nd Annual Workshop on "Economics and Information Security", Berkeley, CA.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. F., & Agarwal, Y. (2015). Your location has been shared 5,398 times! A field study on mobile app privacy nudging. Proceedings of the 33rd annual ACM conference on human factors in computing systems, Seoul, Republic of Korea.

Bandara, H. M. R. J., Fernando, M., & Akter, M. S. (2018). Is the privacy paradox a matter of psychological distance? An exploratory study of the privacy paradox from a construal level theory perspective. Hawaii International Conference on System Sciences, Waikaloa Village, HI.

Bhaskar, R. (2013). *A realist theory of science*. Routledge.

Butori, R., & Miltgen, C. L. (2023). A construal level theory approach to privacy protection: The conjoint impact of benefits and risks of information disclosure. *Journal of Business Research*, *168*.

Cherif, E., Bezaz, N., & Mzoughi, M. (2021). Do personal health concerns and trust in healthcare providers mitigate privacy concerns? Effects on patients' intention to share personal health data on electronic health records. *Social Science & Medicine*, *283*.

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2022). The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychology & Marketing*, *39*(3), 647-661.

Cutcliffe, J. R. (2000). Methodological issues in grounded theory. *Journal of advanced nursing*, *31*(6), 1476-1484.

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy calculus perspective. In *Advances in healthcare informatics and analytics* (pp. 19-50). Springer.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.

Fujita, K., Henderson, M. D., Eng, J., Trope, Y., & Liberman, N. (2006). Spatial distance and mental construal of social events. *Psychological science*, *17*(4), 278-282.

Glaser, B. G., & Strauss, A. L. (2017). *Discovery of grounded theory: Strategies for qualitative research*. Routledge.

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217-227.

Harborth, D., & Pape, S. (2022, June 13–15). A privacy calculus model for contact tracing apps: Analyzing the german corona-warn-app. ICT Systems Security and Privacy Protection: 37th IFIP TC 11 International Conference, SEC, Copenhagen, Denmark.

Hong, J., & Lee, A. Y. (2010). Feeling mixed but not torn: The moderating role of construal level in mixed emotions appeals. *Journal of Consumer Research*, *37*(3), 456-472.

Jerrold, L. (2011). When patients lie to their doctors. *American Journal of Orthodontics and Dentofacial Orthopedics*, *139*(3), 417-418.

Karwatzki, S., Trenz, M., & Veit, D. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. *Information Systems Journal*, *32*(6), 1126-1157.

Keith, M., Clark, A., Masters, T., & Wigington, C. (2022, January 4-7). What makes health data privacy calculus unique? Separating probability from impact. Hawaiian International Conference on System Sciences, Online only.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637-667.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173.

Laibson, D. (1997). Golden eggs and hyperbolic discounting. *The Quarterly Journal of Economics*, *112*(2), 443-478.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22-42.

Levy, A. G., Scherer, A. M., Zikmund-Fisher, B. J., Larkin, K., Barnes, G. D., & Fagerlin, A. (2018). Prevalence of and factors associated with patient nondisclosure of medically relevant information to clinicians. *JAMA network open*, *1*(7), e185293-e185293.

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International journal of medical informatics*, *88*, 8-17.

Liberman, N., & Trope, Y. (2003). Construal level theory of intertemporal judgment and decision.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., & Wells, T. (2012). Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the American Society for Information Science and Technology*, *63*(4), 755-776.

Lustgarten, S. D., Garrison, Y. L., Sinnard, M. T., & Flynn, A. W. P. (2020). Digital privacy in mental healthcare: Current issues and recommendations for technology use. *Current opinion in psychology*, *36*, 25-31.

Masters, T. M., Keith, M., Hess, R., & Jenkins, J. L. (2022). Do privacy assurances work? A study of truthfulness in healthcare history data collection. *PloS one*, *17*(11), e0276442.

MedicareAdvantage.com. (2018). The lies patients and doctors tell: A new patient-doctor communication study. *2020*(July 10th). Retrieved August 2018, from https://www.medicareadvantage.com/patient-doctor-lies-survey

Mehta, R., Zhu, R., & Meyers-Levy, J. (2014). When does a higher construal level increase or decrease indulgence? Resolving the myopia versus hyperopia puzzle. *Journal of Consumer Research*, *41*(2), 475-488.

Mingers, J., Mutch, A., & Willcocks, L. (2013). Critical realism in information systems research. *MIS Quarterly*, *37*(3), 795-802.

Palmieri, J. J., & Stern, T. A. (2009). Lies in the doctor-patient relationship. *Primary care companion to the Journal of clinical psychiatry*, *11*(4), 163.

Panagioti, M., Khan, K., Keers, R. N., Abuzour, A., Phipps, D., Kontopantelis, E., Bower, P., Campbell, S., Haneef, R., Avery, A. J., & Ashcroft, D. M. (2019). Prevalence, severity, and nature of preventable patient harm across medical care settings: Systematic review and meta-analysis. *BMJ*, *366*, l4185.

Shojania, K. G., & Dixon-Woods, M. (2017). Estimating deaths due to medical error: The ongoing controversy and why it matters. *BMJ Quality & Safety*, *26*(5), 423-428.

Singh, T., Johnston, A., Di Gangi, P., & Bott, G. (2018). An examination of risk perceptions and protected health information disclosure intentions: A construal level theory perspective.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individual's concerns about organizational practices. *MIS Quarterly*, *20*(2), 167-196.

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review*, *117*(2), 440.

Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of Consumer Psychology*, *17*(2), 83-95.

Ülkümen, G., & Cheema, A. (2011). Framing goals to influence personal savings: The role of specificity and construal level. *Journal of Marketing Research*, *48*(6), 958-969.

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory' back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal*, *20*(4), 357-381.

Vallacher, R. R., & Wegner, D. M. (1987). What do people think they're doing? Action identification and human behavior. *Psychological Review*, *94*, 3-15.

Vogel, L. (2019). Why do patients often lie to their doctors? In: Can Med Assoc.

Walker, D., & Myrick, F. (2006). Grounded theory: An exploration of process and procedure. *Qualitative health research*, *16*(4), 547-559.

Wegner, D. M., & Vallacher, R. R. (1986). Action identification. In *Handbook of motivation and cognition: Foundations of social behavior*. (pp. 550-582). Guilford Press.

Wiesche, M., Jurisch, M. C., Yetton, P. W., & Krcmar, H. (2017). Grounded theory methodology in information systems research. *MIS Quarterly*, *41*(3), 685-A689.

Witters, D. (2023). U.S. Depression rates reach new highs. *Gallup*. Retrieved September 1st, 2023, from https://news.gallup.com/poll/505745/depression-rates-reach-new-highs.aspx