

Toward Understanding the Technology Trust Calculus in Healthcare: A Generation Z and Millennial View

Mohammed Sajedur Rahman
Emporia State University
mrahman@emporia.edu

Juan A. Chavarria
Emporia State University
jchavar1@emporia.edu

William D. Senn
Emporia State University
wsenn@emporia.edu

Geethalakshmi S. Lakshmikanth
Emporia State University
glakshmi@emporia.edu

Douglass Smith
Emporia State University
dsmith35@emporia.edu

Javier Flores
Emporia State University
jflores6@emporia.edu

Md. Rakibul Hoque
Emporia State University
mhoque@emporia.edu

Abstract

Generation Z and Millennial comprise 50% of the American population and are considered the savviest users of Information Technology (IT). They are also critical beneficiaries of the transformation of healthcare processes and services enabled by IT. Increasingly, the capabilities to leverage digital healthcare depends on the richness of collected data. Consequently, it is imperative to understand the contextual factors that influence Millennial and Gen Z trust in healthcare IT to disclose personal health information. To address this question, we draw on social cognitive theory, social exchange theory, and privacy calculus framework to propose a healthcare technology trust calculus model. We validated it using a survey study collecting responses from 736 individuals. Findings indicate that although the concern of disclosing personal health information negatively influences trust in healthcare IT, organizational trust, perceived benefits, and risks of health information disclosure have a more substantial effect on it.

1. Introduction

Technology is ubiquitous and its applications are growing by the day. This trend of applicability and growth of technology has also come a long way in the Healthcare industry. Younger Americans, Generation (Gen) Z and Millennial, are considered as the most frequent users of technologies. Gen Z who are born in and after 1997 and Millennial born between 1981 and 1996 comprise about 27.7% and 22.03% of the US population, respectively [1], and they are about half of the people living in the US. These generations are known to be keen and quick to adopt new technology, attributing to their

awareness and habits [2]. A recent report provides evidence showing that at least 47% of younger generation uses various forms of healthcare technology and virtual care services, ranging from prescription refill, virtual doctor visits, online test results and diet management, to tracking systems for fitness, health status, and medications [3].

Health information privacy perception and health technology adoption, such as mHealth services, are known to vary across different generations [4, 5]. The need for these information-driven health services poses challenges, redefining healthcare industry. Consumers demand innovative healthcare IT that are both trustworthy and accessible.

With any new technology adoption, it is imperative to understand the antecedent factors that shape the formulation of trust among its users. Technology adoption decisions are often influenced by the age of users. Similarly, trust factors are also perceived differently by different age groups of health technology adopters. A recent study [6] reported that perceptions of risk, trust, and privacy of health information vary among different age groups who adopt healthcare technologies. Furthermore, when exploring antecedents of trust in technology adoption in Information Systems (IS) research, they are commonly categorized according to human-like attributes (e.g., integrity and ability) and system-like attributes (e.g., reliability and usefulness) [7]. Likewise, different studies have shown diverse antecedents when studying technology trust, such as security, privacy, system quality, organizational reputation [8], integrity, ease of use, usefulness, systems and information quality [9], etc., with little to no focus on health or psychological aspects of users.

Therefore, as the level and dynamics of trust changes contextually, there are gaps in existing literature concerning the understanding of individual trust beliefs with regards to healthcare IT. This provides opportunities for new studies, especially in the area of healthcare technology, and specifically for Gen Z and Millennial, where scant knowledge of antecedents of trust is accumulated. In this research, we explore the formation of healthcare technology trust beliefs and investigate their antecedents when applied to healthcare technology. Using theories from IS and Social Psychology literature, we propose a healthcare technology trust calculus model and validate the model by conducting an empirical study.

2. Theoretical Background

Trust has received the attention by researchers from multiple disciplines including social psychology, management, and economics, among others. Various research in economics indicate trust is developed through a calculative process [10], where trustor estimate rewards and costs when placing his/her trust [11]. Trust can be formed in a rational manner following a logical contrast of all possible benefits and risks. Consequently, scholars sustain that trust is the outcome of a calculative process, assessing the costs (often referred to as risks) and benefits before deciding whether to depend on others to achieve a given goal or participate of an exchange [10, 11].

Understanding trust in technology is of the utmost importance if we are to understand why users engage with technology artifacts [12]. Existing Information Systems (IS) literature provides conflicting outcomes when the known formation of trust belief is applied to healthcare context [see for example: 13]. While some recent studies [14] suggest the importance of trust in healthcare technology use, others reported no such relationship [15, 16]. The popular IS theories, “lack in their understanding and descriptive power for potential uses” [17] and, thus, fall short in explaining individuals’ healthcare technology trust behavior. Thus, we explore the social psychology literature to understand psychological mechanisms through which technology trust is formed as trust beliefs incorporate psychological aspect of human behavior. Behavior is often shaped by environmental influences or by internal dispositions [18] and social cognitive theory helps to explain this relationship. Social Cognitive Theory (SCT) [19] is widely used in understanding the formation of human behavior, especially in the adoption, initiation, and maintenance of health behaviors. SCT explains human behavior in terms of psychosocial functioning, where there is triadic reciprocal causation among individuals (dispositional factors), environments (situational factors), and their behaviors [19]. The triad operates as interacting determinants that have bidirectional influences on each other. While SCT has

many dimensions, we are specifically focusing on the role of dispositional and situational factors in forming healthcare technology trust behavior. Thus, we use individuals’ feelings (perceived organizational trust and perceived general privacy concerns) as dispositional factors to understand healthcare technology trust behavior.

SCT also explains that behavioral change is possible by a personal sense of control [20], which can be explained by situational factors. In other words, if individuals believe that they have control over the sensitive health information that they disclose for healthcare technology use, they will more likely have positive change of behavior (trusting belief) toward the technology. To explain the situational factors in healthcare technology trust beliefs, we utilized the Social Exchange Theory (SET) and Privacy Calculus Theory (PCT). A substantial body of extant literature suggest strong relationship between trust belief and privacy belief as exchange of information relies at the heart of these cognitive formations [see for example: 21, 22]. Additionally, both these theories seem to lay foundation for costs-benefits evaluation process needed to establish a relationship, especially in a situation where there is a need for information exchange. Thus, both these theories are important and provide critical theoretical ground in understanding healthcare technology trust calculus as the process involves the exchange of sensitive health and personal information among two parties – healthcare technology and its users. Both SET and PCT were established based on the notion that a relationship between two parties (whether they are individuals, technologies, or organizations) are established through a process of cost-benefit analysis. According to SET, people use a systematic and logical process to determine a balance in their cognitive formation. One of the basic tenets of SET is that a relationship evolves from a trusting belief and parties involved must abide by certain exchange rule(s) [23]. Accordingly, PCT provides the foundation for setting these rule(s) for exchanging information and expectation for both parties.

PCT states that people go through a rational process of evaluation between the benefits and risks of disclosing their personal information. However, in privacy calculus studies, there is an argument against the complete rational assessment. This argument assumes individuals bounded rationality limiting them to process all the applicable and available information required to conduct the privacy calculus [24]. Researchers of privacy calculus argue that the calculative process occurs after an evaluation of situation-specific factors (i.e., perceived risk of information disclosure, perceived health benefits of information disclosure), are limited by dispositional and irrational factors (i.e., perceived general privacy, perceived organizational trust [24]). Further, if the final

net result is considered beneficial, then the person will trust. Thus, building on the theoretical framework proposed by Doney, Cannon and Mullen [10], we argue that situational privacy calculus is the antecedent of trusting healthcare technology.

3. Research Model and Hypotheses

In many social aspects, healthcare, in particular, trust is a precursor and successor to adoption and usage. In the healthcare setting, patients can come into contact and rely upon several entities: healthcare providers (such as physicians, nurses, or other medical staff), healthcare vendors responsible for providing treatment, or various healthcare technologies (medical devices) that are used to provide treatment. Thus, trust among patients, providers, institutions, and healthcare systems is a central tenant of much research [25, 26]. Lack of trust between users and any of the entities, including healthcare technology, leads to the risk of adverse outcomes for patient care [27, 28] as patients refrain from disclosing sensitive health-related information. In this study, we define technology trust as the degree to which people believe that technology will be dependable to protect an individual's personal health information (PHI) [28]. The remaining of this section is used to develop our Healthcare Technology Trust (HTT) Calculus research model as shown in Figure 1 and to discuss the development of related hypotheses.

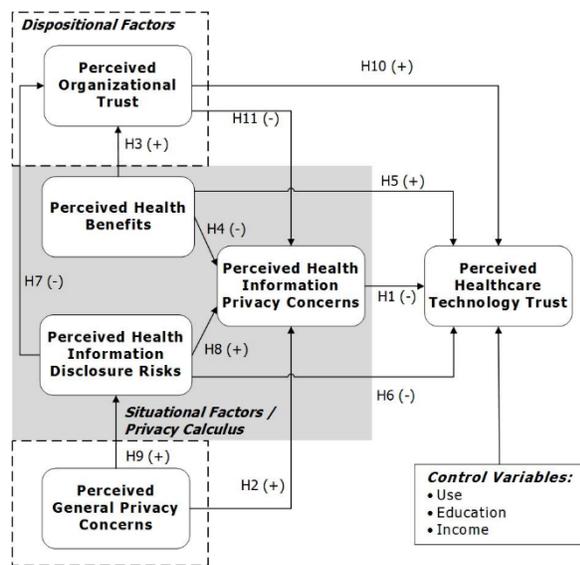


Figure 1. Healthcare Technology Trust (HTT) Calculus Model

3.1. Privacy Concerns

The growing digitization of PHI calls for its robust protection [13]. Despite all the diligent work of healthcare professionals, industry leaders, and scholars, the privacy

protection of PHI remains a critical challenge [29]. In a study with more than 12,000 participants, at least 87% expressed not sharing all their PHI during healthcare appointments [30]. The majority of IS studies on information privacy are focused on general privacy concerns, which is defined as the "individual's general tendency to worry about information privacy" [31]. However, in empirical studies that have used general privacy concerns, scholars have found inconsistent findings [28, 31, 32]. A possible reason for these contradictory findings is that general privacy concerns do not have a specific context, and that could elicit different individual responses [31]. This insight is in line with scholars who advocate for the contextualization of research. Given the healthcare context of this study and suggestions from scholars that information privacy research requires contextualization, we investigate the general and situational context of information privacy. In our model, *general information privacy concerns* tap into the concerns that respondents have while sharing personal information. Additionally, *PHI privacy concerns* tap into the concerns that a respondent has while sharing information related to the specific context of healthcare interaction.

Our research explores the antecedents of technology trust in the healthcare context. Previous IS research on information privacy has underscored the pervasive interrelation between information privacy and trust [33]. Some scholars posit that trust mediates the relationship between information privacy concerns and willingness to disclose private information [32]. Others suggest that trust moderates the influence of privacy concerns on behavior [34], and others propose trust as the antecedent of privacy [35, 36]. In line with previous studies [27, 28], we investigate trust as an outcome of privacy concerns for PHI, which is the cumulative evaluation of the benefits and risks of disclosing PHI reflected in the perceived health information privacy concerns [10]. Consequently, the calculation of health information privacy concerns reduces the disposition to trust toward the technology supporting the delivery of healthcare. As suggested by previous researchers [28], when an individual has a high degree of privacy concerns, they are likely to have low trusting beliefs. For this reason, we put forward the following hypothesis.

H1: Perceived health information privacy concerns negatively influence an individual's trust in Healthcare Information Technology

Further, we acknowledge that the notion of privacy concerns of health information is the result of assessing situational factors and dispositional factors. In the case of dispositional factors, it has been suggested that individuals represent pre-existing attitudes that at a global level reflect the degree to which they have preconceptions that are important to consider in the calculative process

[24] that generates health information privacy concerns. General privacy concerns are about pre-existing apprehensive beliefs that individuals have about how organizations, in general, may misuse their private information. Thus, we hypothesize the following.

H2: General Privacy Concerns positively influence Perceived health information privacy concerns

3.2. Perceived Health Benefits

Individuals make decisions to disclose information considering future consequences by weighing possible positive versus negative outcomes in what is referred to as “calculus of behavior” [37]. People ponder the risk of disclosing personal information against economic or social benefits which is called privacy calculus [38]. This has been studied in the e-Commerce arena, where buyers need to provide personal information to complete transactions. In this environment, consumers evaluate the balance of accepting certain level of risk in favor of positive outcomes [32]. Overall, people presumably will disclose personal information if they perceive they can obtain a positive net result considering risks and benefits in what is known as privacy calculus model [39]. Kim and associates [40] defined perceived benefit as “a consumer’s belief about the extent to which he or she will become better off from the online transaction with a certain website” (p. 547). Correspondingly, we propose the definition of perceived health benefits as a user’s belief about the extent to which he or she will gain health-related benefits from the interaction with technology.

Xu and associates [41] applied an extended privacy calculus model for location-based services involving positioning technologies and providing users with reachability and accessibility as benefits in exchange of their personal information. Within a healthcare context, this risk-benefit analysis would allow users of online services to determine if using these services is worth it. Healthcare consumers consider better doctors’ coordination, a reduction of medical tests, and improved quality of care as possible benefits of health information exchange [42]. In this trade-off of expected benefits and expected risks, users of healthcare websites would consider perceived benefits related to “a reduction in the risk of contracting illnesses and other non-health benefits” [43]. In a study of organizational trust, Mayer et al. [44] describe previous outcomes as an antecedent of trust. This would indicate that past and positive experiences can promote trust on organizations. Moreover, people build trust based on three key characteristics: ability, benevolence, and integrity [45] which apply in the case of most organizations. Organizational trust is reflected on the trust users have on their website when disclosing their personal information to complete transactions. In this scenario, “trust is the

degree to which an organization is perceived to be reliable, competent, benevolent, and to have integrity.” [46]. Therefore, we posit:

H3: Users with higher perceived health benefits will have higher perceived organizational trust.

Considering the trade-off involved in the privacy calculus, higher benefits will counteract risks, reducing their impact on people’s trust [13, 32, 38]. Moreover, the benefits of disclosing PHI may include the convenience of placing orders online [22]. A similar situation within a healthcare environment would mean a decrease in people’s perceived health information privacy concerns. Therefore, we suggest:

H4: Users with higher perceived health benefits will have lower perceived health information privacy concerns.

Patients’ technology trusts in medical settings can be based on three dimensions: technology, care provider, and how the provider uses the technology [26]. Thus, perceived health benefits have a relationship to perceived technology trust that is similar to the one with perceived organizational trust. In other words:

H5: Users with higher perceived health benefits will have higher perceived technology trust.

3.3. Perceived Risks

Risk is an important variable that is used for decision-making purposes in every aspect of human life. People regularly assess risks before making important decisions as well as after the completion of an action. Rohrman and Renn [47] defined the term “risk” as “the possibility that human actions, situations or events might lead to consequences that affect aspects of what humans value” (p. 14). Risk perceptions, on the other hand, provide details about an individual’s judgment about the possibility and magnitude of uncertain consequence(s) associated with his or her action [48, 49]. Van Slyke et al. [21] defined risk perception as individuals’ beliefs regarding the probability of gains or losses associated with their transactions with others. Perceived risk is considered a critical component in establishing relationships [50], which can be social, economic, or even interpersonal relationships between two agents. Over the years, different types of risk perceptions have been used in different areas of research. Huang et al. [48] discuss several kinds of risks, such as financial risk, performance risk, physical risk, psychological risk, and social risk. In this study, we focus on information disclosure risk and its relationship to healthcare technology trust. Thus, risk perception is defined in this study as the extent to which an individual perceives disclosure of PHI as risky.

Understanding risks associated with a system is a major step in understanding and ensuring the safety and security of the system. Just as overestimation of risks can prevent stakeholders from adopting certain technologies,

underestimation of risks associated with technology can promote stakeholders to engage in insecure practices [51]. Risk perceptions play a fundamental role in understanding consumer concerns [52] and users' response behaviors toward different technology threats [51]. Having adequate knowledge of different risks allows individuals to prevent unintended consequences and mitigate harmful effects from the risks. Dinev and Hart [32] used privacy calculus model and social exchange theory to demonstrate that individuals use risk-benefit analysis for their willingness to disclose personal information.

There is strong support for a significant relationship between individuals' risk perceptions and their trust and acceptance of electronic services. For example, Sztompka [53] reported a dichotomous relationship between risk perception and trust such that low trust can make the situation risky and high trust can totally nullify the risk. On the other hand, other researchers [e.g. 54, 55] viewed the relationship as degree of effects such that the degree of trust affects the level and degree of an individual's risk belief. While IS researchers have made major strides in understanding and quantifying consumer-related risks, few have focused on health-related information disclosure risks and their association with technology trust. Eiser et al. [56] reported a negative correlation between risk perception and trust such that a high level of risk perception contributes to a lower level of technology trust. A study by Rohm & Milne [57] revealed that health information (i.e., medical history) is more sensitive than other types of information (i.e., financial history), and thus people evaluate health information risks at a much higher level and are more sensitive about disclosing their health information. They reported a significant relationship between trust and risk in health information disclosure. Bansal et al. [27] investigated the impact of risk perceptions on individuals' willingness to disclose PHI on health websites and found that individuals' risk beliefs negatively affect their trusts toward the system and level of trust in turn, affects their intention to disclose PHI. Anderson and Agarwal [13] conducted an empirical study and found that risk factors have significant influence on trust in electronic medium in shaping individuals' willingness to provide access to their PHI. Based on these evidences in the existing literature, we posit the following hypotheses.

H6: Health Information Disclosure Risk Perception negatively influences an individual's technology trust perception.

H7: Health Information Disclosure Risk Perception negatively influences an individual's organizational trust perception.

Information privacy concerns are believed to be associated with individuals' risk perceptions. In fact, individuals' risk perceptions, in many situations, act as a

consequence of their privacy concerns [58] such that organizations who collect consumers' personal information for routine business purposes generally try to implement privacy policies and disclose fair information practices to lower consumer privacy concerns, which in turn minimize their risk perceptions. Often time individuals' perceived risk has been shown as an antecedent of their information privacy concerns such that perceived risk affects their concerns for information privacy [see for example: 59]. Individuals generally conduct risk calculations prior to disclosing their personal information. This process of risk calculation involves assessing the likelihood of suffering negative consequences to gauge their level of privacy concern [60]. Milne and Culnan [61] found privacy notices to be an important factor affecting consumers' risk perceptions and reducing their privacy concerns. Individuals' information privacy concerns influence how the person perceives disclosing personal information as risky [28]. Thus, privacy concerns have been widely supported to have a very close interrelationship with risk perceptions.

Malhotra et al. [28] investigated the relationship between internet users' information privacy concerns and their risk beliefs on disclosing personal information online and found a significant positive relationship such that higher internet users' information privacy concerns leads to high level of risk beliefs toward disclosing their personal information online. Other studies [21, 59] also found a similar and positive relationship between risk beliefs and privacy concerns. Despite having a fair amount of research focusing on privacy concerns and their relation to information disclosure risk, we found no study focusing on this relationship in the context of privacy and risks associated with health information disclosure. However, we believe that the positive relationship between privacy concerns and information disclosure risk holds true in the healthcare context. Thus, we posit the following hypotheses.

H8: Health Information Disclosure Risk Perception positively influences an individual's health information privacy concern perception.

H9: General privacy concern perception positively influences an individual's health information disclosure risk perception.

3.4. Perceived Organizational Trust

Trust facilitates efficient business transactions and increases customer satisfaction [62]. It is because of this high impact of trust in an organizational context, there has been a lot of work in literature exploring the foundations of Organizational trust [63]. Rousseau et al. [64] defined trust as the psychological willingness of a party to be vulnerable to the actions of another party (individual or

organization) based on positive expectations regarding the other party's motivation and/or behavior. Often it is seen that organizational trust has been described in terms of the trustor, the trustee, and the risk factor where the trustor's perception of privacy with the organization is an important factor in estimating the organizational trust [44]. So, the lesser the trustor's concern of privacy, the greater the organizational trust. The organizational trust in the healthcare industry has been studied with respect to a technological advancement named 'eDiaMoND' and clearly outlines the ethical concerns associated with information storage, privacy, and security [65]. The research acknowledges that affording trust and providing enough trust with respect to handling sensitive data is the biggest challenge faced by the e-health and e-science systems [65].

A very clear connection between Organizational trust and Technology trust, when applied to the healthcare industry, is described by an Extended Technology Acceptance Model in [15]. Another study [66] found that the antecedents of trust in technology attributed to the Company. Yet another study by Rohm & Milne [57] suggests that having trust in an organization is important in reducing medical information privacy concerns and for disclosing PHI. Thus, we posit the following hypotheses:

H10: Perceived Organizational Trust positively influences an individual's perceived healthcare technology trust.

Organizations are increasingly collecting a huge amount of data from customers to help serve them better and use efficient marketing strategies, especially in the healthcare industry. However, collecting adequate data requires clients or patients' willingness to disclose their personal information. Studies suggest people's privacy concerns about their personal information is directly tied to how they view institutions' privacy policies [60]. Palmer et al. [67] reported that organizations deliberately promote trusting components via websites to minimize the privacy concerns of potential clients. Furthermore, the study suggests that customers are willing to disclose personal information and have the organization use that information only when their concerns about privacy are addressed by the organization's fair procedures [38]. Based on these evidences in existing literature, we posit the following hypothesis.

H11: Perceived Organizational Trust negatively influences an individual's Perceived Health Information Privacy Concerns.

4. Methodology

We used a survey methodology for assessing the proposed research model for healthcare technology trust. The survey used a 5-point Likert scale with 1 for strongly

disagree, and 5 representing strongly agree for all questions. We contextualized the construct using validated survey items from prior research. Table 1 shows the constructs and the source from which they were adapted. Questions were rephrased to fit the context of this study. Data was collected using participants from college students. A call for a survey was sent out, and a total of 736 respondents completed the online survey over a period of 4 weeks. College students are an appropriate population for this study as the focus of this study is to understand the formation of technology trust among Gen Z and Millennial. Additionally, younger population between 21 to 30 years of age are the largest users of Internet and web-based technologies and, thus, using college students to understand technology-related trust is ideal.

5. Data Analysis and Results

The purpose of the current study is to investigate trust in healthcare technology and the factors influencing that trust in Gen Z and Millennial. To facilitate an analysis of healthcare technology trust, the authors developed the aforementioned HTT research model comprised of Perceived Health Benefits, Perceived Health Information Disclosure Risks, Perceived General Privacy Concerns, Perceived Organizational Trust, Perceived Health Information Privacy Concerns, Perceived Healthcare Technology Trust, and four control variables - Age, Income, Education, and Number of Device Use.

Table 1. Construct Reliability and Validity

Constructs	Cronbach's α	AVE	Composite Reliability	Items [Source]
GPC	0.781	0.820	0.901	2 [68]
OT	0.816	0.732	0.891	3 [45]
HB	0.924	0.767	0.943	3 [39]
HIDR	0.836	0.753	0.902	3 [39]
HIPC	0.912	0.793	0.939	4 [69]
HTT	0.876	0.730	0.915	4 [70]

Note: HB- Health Benefits; HIPC- Health Information Privacy Concerns; HTT- Health Technology Trust; HIDR- Health Information Disclosure Risk; OT- Organizational Trust; GPC- General Privacy Concern.

Our analysis used SmartPLS 3 [71]. We first evaluated the reliability and validity of the measurement model before analyzing the structural model. The convergent validity of the variables was ensured by confirming that all items were loaded to the respective construct with factor loadings that are much higher than the recommended threshold of 0.5. To evaluate the

construct reliability, we examined three measures. The Cronbach's alpha for each of the constructs ranges from 0.78 to 0.92 and composite reliability ranges from 0.89 to 0.94, exceeding the minimum recommended threshold of 0.7 for both reliability measures. The range for average variant extracted (AVE) is 0.73 to 0.82, also exceeding the recommended threshold of 0.5. Table 1 provides the actual value for each of the reliability measurements. The discriminant validity was assessed by ensuring that the square root of AVE values is higher than the inter-construct correlation, as shown in table 2. Finally, we tested for common method bias issues using collinearity statistics, and all the variance inflation factor (VIF) values at the factor level are much less than the recommended threshold of 3.3, indicating common method bias does not exist in our instrument.

Table 2. Discriminant Validity

	GPC	OT	HIPC	HB	HIDR	HTT
GPC	0.906					
OT	-0.272	0.855				
HIPC	0.643	-0.268	0.890			
HB	-0.151	0.420	-0.191	0.876		
HIDR	0.557	-0.316	0.614	-0.259	0.868	
HTT	-0.210	0.561	-0.240	0.426	-0.245	0.854

All results confirm that the measurement constructs are valid and reliable. A structural model was developed and measured to test the hypothetical model. A summary of path values and significance is available in Table 3. Two variables were shown to have a positive influence on Perceived Healthcare Technology Trust ($R^2 = 0.374$), namely, Perceived Health Benefits ($\beta = 0.23$, $p < 0.000$) and Perceived Organizational Trust ($\beta = 0.441$, $p < 0.000$), leading support to H5 and H10. Perceived Health Information Privacy Concerns had a slight negative influence ($\beta = 0.078$, $p = 0.046$) on Technology Trust, supporting H1, whereas Perceived Health Information Disclosure Risks was hypothesized to have a positive influence, but was not found to be significant. Thus, no support for H6 was found.

Perceived Health Information Privacy Concern, an antecedent of Perceived Healthcare Technology Trust, was hypothesized to be influenced by four variables ($R^2 = 0.510$); Perceived Health Benefits, Perceived Health Information Disclosure Risks, Perceived General Privacy Concerns, and Perceived Organizational Trust. Two of the four antecedents, Perceived Health Information Disclosure Risks ($\beta = 0.359$, $p < 0.000$) and Perceived General Privacy Concerns ($\beta = 0.432$, $p < 0.000$) were found to be significant, supporting H2 and H8, respectively. No significance was found for the paths Perceived Health Benefits and Perceived Organizational Trust, rejecting H4 and H11, respectively. Perceived Organizational trust ($R^2 = 0.222$) is influenced by

Perceived Health Information Disclosure Risk ($\beta = -0.222$, $p < 0.000$) and Perceived Health Benefits ($\beta = -0.362$, $p < 0.000$), supporting both H3 and H7, respectively. Perceived Health Information Disclosure Risk ($R^2 = 0.311$) is influenced by Perceived General Privacy Concerns ($\beta = 0.557$, $p < 0.000$), supporting H9. Finally, the control variables had little impact on Perceived Healthcare Technology Trust. Number of Devices Used was not significant ($p < 0.070$), and neither was Education ($p < 0.834$) Income had a small negative influence ($\beta = -0.081$, $p < 0.006$).

Table 3. Hypotheses Test Results

	PATH	Dir.	β (p)	Supp.
H1	HIPC \rightarrow HTT	-	-0.078 (0.046)	Yes
H2	GPC \rightarrow HIPC	+	0.432 (0.000)	Yes
H3	HB \rightarrow OT	+	0.362 (0.000)	Yes
H4	HB \rightarrow HIPC	-	-0.022 (0.539)	No
H5	HB \rightarrow HTT	+	0.230 (0.000)	Yes
H6	HIDR \rightarrow HTT	-	0.002 (0.955)	No
H7	HIDR \rightarrow OT	-	-0.222 (0.000)	Yes
H8	HIDR \rightarrow HIPC	+	0.359 (0.000)	Yes
H9	GPC \rightarrow HIDR	+	0.548 (0.000)	Yes
H10	OT \rightarrow HTT	+	0.441 (0.000)	Yes
H11	OT \rightarrow HIPC	-	-0.027 (0.457)	No

6. Discussion of Results

This research addresses the determinants of trust in healthcare information technology. A healthcare technology trust calculus model was proposed and validated. The results revealed several dispositional and situational factors that are important in shaping an individual's trust belief in healthcare technology. We found that health benefits, health information privacy concerns, and organizational trust perceptions are all important antecedent factors for technology trust. Among all the antecedents of healthcare technology trust belief, organizational trust seems to have the strongest influence ($\beta=0.441$, $T=10.875$) on trust belief followed by health benefits ($\beta=0.230$, $T=5.910$).

Contrary to our expectations from the privacy calculus theory, where individuals evaluate benefits and risks on forming trust belief, we only see the benefits of having a significant influence. It seems perceived health technology trust is mainly influenced by positive constructs such as perceived health benefits and perceived organizational trust. Constructs involving concerns and risks, such as perceived health information disclosure risks and perceived health information privacy

concerns show no significant influence and weak influence on technology trust, respectively. This finding further suggests that Gen Z and Millennial tend to trust technology more than organizations as health information disclosure risk is not important for technology trust (insignificant) but important (significant) on organizational trust and privacy concerns.

The results revealed an interesting finding with regards to privacy calculus. In privacy calculus theory, perceived benefits and risks are expected to form an individual's privacy concerns. However, the results suggest that the typical costs-benefits analysis does not hold true when it comes to privacy concerns related to PHI. In other words, knowledge of health benefits of disclosing PHI does not minimize privacy concerns. On the other hand, individuals' knowledge about Health benefits significantly improves their trust in healthcare technology and healthcare organization. We also found that health information privacy concerns mediate the relationship between risk perception and technology trust such that risk perceptions influence health information privacy concerns, which in turn influences healthcare technology trust perceptions. The results further show the significance of both health information privacy concerns and health benefits perceptions as antecedents of trust, which implies that the knowledge of health benefits of disclosing PHI does not alleviate individuals' concerns for health information privacy. Finally, income was found as a significant control variable implying its influence on technology trust beliefs.

7. Implications and Limitations

This study enables a thorough understanding of healthcare technology trust and its antecedents, thereby helping us to understand the implications of healthcare technology growth. Consequently, the aim of this study is to explore and identify the strong antecedents of Trust in healthcare technology context among the Gen Z and Millennial. This is a significant study given that these population groups are considered digital natives, and their levels of trust, attitudes, and concerns with healthcare technology adoption are likely to vary considerably from other generations.

Our study has several limitations that must be acknowledged. First, we used students as respondents. Although students could be considered appropriate respondents of technology adoption research involving Gen Z and Millennial, the results may not be generalizable. Future studies can include non-student population, which may lead to better generalizability of the findings. Second, the majority of our survey responses are from one educational institution, which may contribute to the homogeneity of the responses. Future

studies should consider participants from different institutions or different geographical regions. Third, we used self-reported surveys. Although self-reported surveys are widely used in technology adoption research, it contributes to many different biases in the study results [72]. Future studies can use other methods to avoid these biases or should take appropriate steps to mitigate some of these biases.

8. Conclusion

In this study, we identified gaps in existing literature in understanding how trust beliefs are formulated for healthcare technology, specifically for Gen Z and Millennial. To fill this void, we proposed a healthcare technology trust calculus model grounded on theories from both IS and Psychology literature. Several interesting findings were revealed. We reported several dispositional and situational factors that are important antecedents in the formation of healthcare technology trust beliefs. The results suggest that typical privacy calculus does not hold true for younger generation (Gen Z and Millennial) in the healthcare technology context. The results further suggest that although health information privacy concerns is an important antecedent, organizational trust and health benefits perceptions have greater influences on forming trust beliefs for healthcare technologies. We believe that these findings are unique, interesting, and an important step forward in understanding people attitudes toward healthcare technologies.

9. References

- [1] Duffin, E.: Statista Report - 'U.S. Population by generation 2018', 2020
- [2] Pennic, J.: Accenture Survey Report - 'Millennials and gen z embracing virtual care models', 2019
- [3] Cohen, J.K.: Becker's Hospital Review Report - '5 ways all generations — from millennials to seniors — are adopting virtual care', 2018
- [4] Kenny, G., and Connolly, R.: 'Towards an inclusive world: Exploring m-health adoption across generations', Twenty-Fifth European Conference on Information Systems (ECIS), 2017
- [5] Guo, X., Zhang, X., and Sun, Y.: 'The privacy–personalization paradox in mhealth services acceptance of different age groups', *Electronic Commerce Research and Applications*, 2016, 16, pp. 55-65
- [6] Fox, G., and Connolly, R.: 'Mobile health technology adoption across generations: Narrowing the digital divide', *Information Systems Journal*, 2018, 28, (6), pp. 995-1019
- [7] Lankton, N.K., McKnight, D.H., and Tripp, J.: 'Technology, humanness, and trust: Rethinking trust in technology', *Journal of the Association for Information Systems*, 2015, 16, (10), pp. 1

- [8] Zaman, Y., Jamil, R., and Kazmi, Z.: 'Antecedents of trust in online environment: A case of Pakistan', *Management Science Letters*, 2016, 6, (3), pp. 193-202
- [9] Van Deventer, M.: 'Antecedents of trust in mobile banking amongst generation y students in South Africa', *Acta Universitatis Danubius. (Economica)*, 2019, 15, (3)
- [10] Doney, P.M., Cannon, J.P., and Mullen, M.R.: 'Understanding the influence of national culture on the development of trust', *Academy of management review*, 1998, 23, (3), pp. 601-620
- [11] Williamson, O.E.: 'Calculativeness, trust, and economic organization', *The journal of law and economics*, 1993, 36, (1, Part 2), pp. 453-486
- [12] Gefen, D., Benbasat, I., and Pavlou, P.: 'A research agenda for trust in online environments', *Journal of Management Information Systems*, 2008, 24, (4), pp. 275-286
- [13] Anderson, C.L., and Agarwal, R.: 'The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information', *Information Systems Research*, 2011, 22, (3), pp. 469 - 490
- [14] Xiao, N., Sharman, R., Rao, H., and Upadhyaya, S.: 'Factors influencing online health information search: An empirical analysis of a national cancer-related survey', *Decision Support Systems*, 2014, 57, pp. 417 - 427
- [15] Terrizzi, S., Sherer, S., Meyerhoefer, C., Scheinberg, M., and Levick, D.: 'Extending the technology acceptance model in healthcare: Identifying the role of trust and shared information', 2012
- [16] Xie, H., Prybutok, G., Peng, X., and Prybutok, V.: 'Determinants of trust in health information technology: An empirical investigation in the context of an online clinic appointment system', *International Journal of Human-Computer Interaction*, 2020, 36, (12), pp. 1095-1109
- [17] Oinas-Kukkonen, H.: 'A foundation for the study of behavior change support systems', *Personal and ubiquitous computing*, 2013, 17, (6), pp. 1223-1235
- [18] Bandura, A.: 'Social cognitive theory of mass communication', *Media psychology*, 2001, 3, (3), pp. 265-299
- [19] Bandura, A.: 'Social foundations of thought and action: A social cognitive theory' (Prentice-Hall Englewood Cliffs, NJ, 1986)
- [20] Luszczynska, A., and Schwarzer, R.: 'Social cognitive theory', *Predicting health behaviour*, 2005, 2, pp. 127-169
- [21] Van Slyke, C., Shim, J., Johnson, R., and Jiang, J.: 'Concern for information privacy and online consumer purchasing', *Journal of the Association for Information Systems*, 2006, 7, (6), pp. 415 - 444
- [22] Smith, H.J., Dinev, T., and Xu, H.: 'Information privacy research: An interdisciplinary review', *MIS Quarterly*, 2011, 35, (4), pp. 989 - 1015
- [23] Cropanzano, R., and Mitchell, M.S.: 'Social exchange theory: An interdisciplinary review', *Journal of management*, 2005, 31, (6), pp. 874-900
- [24] Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E.: 'Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus', *Information Systems Journal*, 2015, 25, (6), pp. 607-635
- [25] Montague, E.: 'Validation of a trust in medical technology instrument', *Applied Ergonomics*, 2010, 41, (6), pp. 812-821
- [26] Montague, E., and Asan, O.: 'Trust in technology-mediated collaborative health encounters: Constructing trust in passive user interactions with technologies', *Ergonomics*, 2012, 55, (7), pp. 752-761
- [27] Bansal, G., Zahedi, F., and Gefen, D.: 'The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online', *Decision Support Systems*, 2010, 49, (2), pp. 138 - 150
- [28] Malhotra, N.K., Kim, S.S., and Agarwal, J.: 'Internet users' information privacy concerns (iupc): The construct, the scale, and a causal model', *Information Systems Research*, 2004, 15, (4), pp. 336 - 355
- [29] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, accessed July 1 2020
- [30] Alder, S.: 'Patients holding back health information over data privacy fears', in Editor (Ed.) (Eds.): 'Book Patients holding back health information over data privacy fears' (2017, edn.), pp.
- [31] Li, H., Sarathy, R., and Xu, H.: 'The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors', *Decision Support Systems*, 2011, 51, (3), pp. 434 - 445
- [32] Dinev, T., and Hart, P.: 'An extended privacy calculus model for e-commerce transactions', *Information Systems Research*, 2006, 17, (1), pp. 61 - 80
- [33] Pavlou, P.A.: 'State of the information privacy literature: Where are we now and where should we go', *MIS quarterly*, 2011, 35, (4), pp. 977-988
- [34] Bansal, G., and Zahedi, F.: 'The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation', *ICIS 2008 Proceedings*, 2008, pp. 7
- [35] Belanger, F., Hiller, J.S., and Smith, W.J.: 'Trustworthiness in electronic commerce: The role of privacy, security, and site attributes', *The Journal of Strategic Information Systems*, 2002, 11, (3), pp. 245 - 270
- [36] Eastlick, M.A., Lotz, S.L., and Warrington, P.: 'Understanding online b-to-c relationships: An integrated model of privacy concerns, trust, and commitment', *Journal of Business Research*, 2006, 59, (8), pp. 877-886
- [37] Stone, E.F., and Stone, D.L.: 'Privacy in organizations: Theoretical issues, research findings, and protection mechanisms', *Research in Personnel and Human Resources Management*, 1990, 8, (3), pp. 349 - 411
- [38] Culnan, M.J., and Armstrong, P.K.: 'Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation', *Organization Science*, 1999, 10, (1), pp. 104 - 115
- [39] Dinev, T., Xu, H., Smith, J.H., and Hart, P.: 'Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts', *European Journal of Information Systems*, 2013, 22, (3), pp. 295-316
- [40] Kim, D.J., Ferrin, D.L., and Rao, H.R.: 'A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents', *Decision Support Systems*, 2008, 44, (2), pp. 544 - 564
- [41] Xu, H., Teo, H.-H., Tan, B.C., and Agarwal, R.: 'The role of push-pull technology in privacy calculus: The case of location-based services', *Journal of Management Information Systems*, 2009, 26, (3), pp. 135 - 174

- [42] Dimitropoulos, L., Patel, V., Scheffler, S.A., and Posnack, S.: 'Public attitudes toward health information exchange: Perceived benefits and concerns', *American Journal of Managed Care (AJMC)*, 2011, 17, (Special Issue), pp. SP111 - SP116
- [43] Huang, J.-C.: 'Remote health monitoring adoption model based on artificial neural networks', *Expert Systems with Applications*, 2010, 37, (1), pp. 307 - 314
- [44] Mayer, R.C., Davis, J.H., and Schoorman, F.D.: 'An integrative model of organizational trust', *Academy of management review*, 1995, pp. 709-734
- [45] Pirson, M., and Malhotra, D.: 'Foundations of organizational trust: What matters to different stakeholders?', *Organization Science*, 2011, 22, (4), pp. 1087-1104
- [46] Metzger, M.J.: 'Privacy, trust, and disclosure: Exploring barriers to electronic commerce', *Journal of Computer-Mediated Communication*, 2004, 9, (4)
- [47] Rohrmann, B., and Renn, O.: 'Risk perception research', in Renn, O., and Rohrmann, B. (Eds.): 'Cross-cultural risk perception' (Kluwer Academic Publishers, 2000), pp. 11-53
- [48] Huang, W.y., Schrank, H., and Dubinsky, A.J.: 'Effect of brand name on consumers' risk perceptions of online shopping', *Journal of Consumer Behaviour*, 2004, 4, (1), pp. 40-50
- [49] Mitchell, V.-W.: 'Consumer perceived risk: Conceptualisations and models', *European Journal of marketing*, 1999, 33, (1/2), pp. 163-195
- [50] Song, J., and Zahedi, F.: 'Trust in health intermediaries', *Decision Support Systems*, 2007, 43, (2), pp. 390-407
- [51] Huang, D.-L., Rau, P.-L.P., and Salvendy, G.: 'Perception of information security', *Behaviour & Information Technology*, 2010, 29, (3), pp. 221 - 232
- [52] Cazier, J.A., Jensen, A.S., and Dave, D.S.: 'The impact of consumer perceptions of information privacy and security risks on the adoption of residual rfid technologies', *Communications of the Association for Information Systems*, 2008, 23, (14), pp. 235 - 256
- [53] Sztompka, P.: 'Trust: A sociological theory' (Cambridge University Press, 1999)
- [54] Jarvenpaa, S.L., Knoll, K., and Leidner, D.E.: 'Is anybody out there? Antecedents of trust in global virtual teams', *Journal of management information systems*, 1998, 14, (4), pp. 29-64
- [55] Jarvenpaa, S.L., Tractinsky, N., and Saarinen, L.: 'Consumer trust in an internet store: A cross-cultural validation', *Journal of Computer-Mediated Communication*, 1999, 5, (2)
- [56] Eiser, J.R., Miles, S., and Frewer, L.J.: 'Trust, perceived risk, and attitudes toward food technologies', *Journal of Applied Social Psychology*, 2002, 32, (11), pp. 2423-2433
- [57] Rohm, A.J., and Milne, G.R.: 'Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern', *Journal of Business Research*, 2004, 57, (9), pp. 1000 - 1011
- [58] Li, Y.: 'Empirical studies on online information privacy concerns: Literature review and an integrative framework', *Communications of the Association for Information Systems*, 2011, 28, (1), pp. 453 - 496
- [59] Liao, C., Liu, C.-C., and Chen, K.: 'Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model', *Electronic Commerce Research and Applications*, 2011, 10, (6), pp. 702-715
- [60] Xu, H., Dinev, T., Smith, J., and Hart, P.: 'Information privacy concerns: Linking individual perceptions with institutional privacy assurances', *Journal of the Association for Information Systems*, 2011, 12, (12), pp. 798 - 824
- [61] Milne, G.R., and Culnan, M.J.: 'Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices', *Journal of Interactive Marketing*, 2004, 18, (3), pp. 15 - 29
- [62] Nootboom, B.: 'Trust, opportunism and governance: A process and control model', *Organization studies*, 1996, 17, (6), pp. 985-1010
- [63] Kramer, R.M.: 'Trust and distrust in organizations: Emerging perspectives, enduring questions', *Annual review of psychology*, 1999, 50, (1), pp. 569-598
- [64] Rousseau, D.M., Sitkin, S.B., Burt, R.S., and Camerer, C.: 'Not so different after all: A cross-discipline view of trust', *Academy of management review*, 1998, 23, (3), pp. 393-404
- [65] Jirotko, M., Procter, R., Hartswood, M., Slack, R., Simpson, A., Coopmans, C., Hinds, C., and Voss, A.: 'Collaboration and trust in healthcare innovation: The ediamond case study', *Computer Supported Cooperative Work (CSCW)*, 2005, 14, (4), pp. 369-398
- [66] Söderström, E., Eriksson, N., and Åhlfeldt, R.-M.: 'Managing healthcare information: Analyzing trust', *International journal of health care quality assurance*, 2016
- [67] Palmer, J.W., Bailey, J.P., and Faraj, S.: 'The role of intermediaries in the development of trust on the www: The use and prominence of trusted third parties and privacy statements', *Journal of Computer-Mediated Communication*, 2000, 5, (3), pp. JCMC532
- [68] Schwaig, K.S., Segars, A.H., Grover, V., and Fiedler, K.D.: 'A model of consumers' perceptions of the invasion of information privacy', *Information & Management*, 2013, 50, (1), pp. 1 - 12
- [69] Boysen, S., Hewitt, B., Gibbs, D., and McLeod, A.: 'Refining the threat calculus of technology threat avoidance theory', *Communications of the Association for Information Systems*, 2019, 45, (1), pp. 5
- [70] McKnight, D.H., Choudhury, V., and Kacmar, C.: 'The impact of initial consumer trust on intentions to transact with a web site: A trust building model', *The Journal of Strategic Information Systems*, 2002, 11, (3), pp. 297-323
- [71] Ringle, C.M., Wende, S., and Will, A.: '"Smartpls 3." Boenningstedt: Smartpls gmbh', in Editor (Ed.) (Eds.): 'Book "Smartpls 3." Boenningstedt: Smartpls gmbh' (Hamburg, Germany, 2015, edn.), pp.
- [72] Williams, P.A., Jenkins, J., Valacich, J., and Byrd, M.D.: 'Measuring actual behaviors in hci research—a call to action and an example', *AIS Transactions on Human-Computer Interaction*, 2017, 9, (4), pp. 339-352