Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Perceived Behavioral Data Utilization and Trust in Human-Centric Digital Health Systems

Faisal Binsar

faisal.binsar@binus.ac.id

Bina Nusantara University

Erwin Tenggono

Pelita Harapan University

Dewi Sri Surya Wuisan

Pelita Harapan University

Research Article

Keywords: Behavioral data utilization, Digital health, Digital health trust, Human-centric systems, Personalization, User trust

Posted Date: November 12th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11251424/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Perceived Behavioral Data Utilization and Trust in Human-Centric Digital Health Systems

Article type: Research Article

Faisal Binsar
Management Department, Binus Online Leraning, Bina Nusantara University, and Research Interest Group in Educational Technology, Bina Nusantara University, Jakarta 11480, Indonesia
ORCID: 0000-0003-1173-5603
Email: faisal.binsar@binus.ac.id *(Corresponding author)*

Erwin Tenggono
Department of Hospital Administration, Graduate School of Medicine, Pelita Harapan University, Tangerang, Indonesia;
Faculty of Economics and Business, Universitas Indonesia, Jakarta, Indonesia
ORCID: 0000-0001-6607-9442
Email: erwin.tenggono@lecturer.uph.edu

Dewi Sri Surya Wuisan
Department of Hospital Administration, Graduate School of Medicine, Pelita Harapan University, Tangerang, Indonesia.
ORCID: 0000-0001-8550-3659
Email: dewi.wuisan@uph.edu

Corresponding author:
Faisal Binsar (Email: faisal.binsar@binus.ac.id)

Abstract: The increasing use of behavioral and personal data has become central to the delivery of personalized digital-health services. Although previous research has extensively examined privacy concerns, data sharing, and technology acceptance, less attention has been given to how users perceive the broader process through which behavioral data are collected, processed, and utilized, and how these perceptions relate to trust in human-centric digital health systems. This study addresses this gap by examining the association between Perceived Behavioral Data Utilization (PBDU) and Digital Health Trust (DHT). Data were collected through a cross-sectional online survey, yielding 485 valid responses. PBDU was measured across data collection, data processing, and data utilization, while DHT was assessed through integrity, benevolence, and competence. Data were processed and analyzed using Python in a Jupyter Notebook environment. Descriptive statistics, Cronbach's alpha, and Pearson's correlation were employed. The findings show consistently high perceptions of behavioral-data utilization across the nine PBDU items, with mean scores ranging from 3.934 to 4.113. DHT likewise demonstrated favorable evaluations, with item means ranging from 3.899 to 4.027. Both

constructs demonstrated high internal consistency, with Cronbach's alpha values of 0.897 for PBDU and 0.909 for DHT. Pearson's analysis identified a positive association between PBDU and DHT ($r = 0.440$, $p < 0.001$). The findings indicate that users' recognition of behavioral-data utilization can coexist with relatively high trust in digital-health systems. The study contributes a data-utilization perspective to the human-centric understanding of trust in personalized digital health, complementing conventional privacy-centered approaches.

Keywords: Behavioral data utilization; Digital health; Digital health trust; Human-centric systems; Personalization; User trust

1. Introduction

Digital health is increasingly becoming a data-intensive form of healthcare delivery in which digital platforms do more than provide access to information or facilitate communication between users and health professionals [1]. The growing integration of mobile applications, health information systems, remote monitoring, and intelligent services enables platforms to continuously generate, collect, and process information about users [2]. Behavioral traces, interaction histories, and health-related information can subsequently be transformed into personalized recommendations and other user-specific services [3]. This shift creates substantial opportunities for more responsive and individualized healthcare, but it also makes the management and interpretation of personal data an increasingly important part of the digital-health experience. Recent research emphasizes that data-driven digital health simultaneously raises opportunities for personalization and concerns regarding privacy, security, transparency, and trust [4].

The central challenge is therefore not simply whether digital-health platforms collect personal data, but whether users recognize how those data are utilized [5]. Data collection is only the initial stage of a broader process in which information may be analyzed, combined, interpreted, and translated into personalized services. When this process becomes visible through tailored recommendations or individualized health functions, users may perceive data utilization as a source of value [6]. At the same time, greater awareness of data use may heighten concerns about privacy, secondary use, and loss of control [7], [8]. This tension is particularly important in digital health because the information involved may be considerably more sensitive than conventional consumer data [9], [10]. Recent evidence shows that consumers' willingness to share digital health information is associated not only with consent but also with transparency, oversight, and mechanisms that strengthen users' control over their information [3].

Trust consequently occupies a critical position in the relationship between users and data-driven digital-health platforms. Users must make judgments about whether platforms are capable of managing their information, whether their interests are

adequately considered, and whether stated commitments concerning data protection and responsible use can be relied upon. Recent empirical research has demonstrated that trust is closely connected with privacy and personalization in smart healthcare. Liu and Tao [11], for example, found that personalization and perceived loss of privacy were important factors associated with public acceptance of smart healthcare, with trust playing a central role in these relationships. Similarly, research on health information exchange indicates that individuals evaluate both the benefits and risks of sharing personal health information, with information security, perceived benefits, and the nature of the receiving organization shaping trust and willingness to share [2], [8].

Despite this growing literature, an important gap remains. Existing studies have predominantly examined privacy concerns, perceived risks, consent, personalization, data sharing, or technology acceptance as separate determinants of digital-health trust or adoption [8]. Less attention has been given to users' perceptions of the broader utilization of behavioral data itself (from data collection and processing to the perceived use of those data to improve digital-health services) and how such perceptions correspond with trust. This distinction matters because users may not interpret data utilization exclusively as a privacy threat. They may also regard it as evidence that a platform is capable of understanding their needs and delivering relevant services. The resulting relationship may therefore be more nuanced than a simple assumption that greater data utilization necessarily reduces trust.

This study addresses this gap by introducing Perceived Behavioral Data Utilization (PBDU) as a focal construct encompassing users' perceptions of behavioral-data collection, processing, and utilization, and examining its association with Digital Health Trust (DHT) [12]. DHT is considered multidimensionally through perceptions of integrity, benevolence, and competence. Rather than testing whether data utilization causes trust, the study investigates whether users who perceive stronger behavioral-data utilization also tend to report stronger trust in digital-health platforms. This approach is particularly relevant because contemporary digital-health systems increasingly depend on continuous data flows to deliver personalized services, while trust remains essential for sustained user engagement and data sharing. Recent work on health-app trust likewise demonstrates that privacy control, trust, and provider characteristics remain important in shaping users' intentions to engage with digital-health services [3], [13].

The study makes three contributions. First, it contributes conceptually by shifting attention from the conventional privacy-risk perspective toward users' perceptions of behavioral-data utilization as a multidimensional process. This perspective recognizes that data practices can simultaneously represent potential risk and perceived service value. Second, it contributes empirically by examining the PBDU–DHT association using survey evidence from digital-health users, thereby providing descriptive evidence on how visible data utilization is within users' platform experiences and how it corresponds with

trust. Third, it contributes practically by highlighting that trust in data-driven digital health may depend not only on protecting information but also on how clearly and credibly platforms demonstrate the purpose and value of data utilization.

Accordingly, this study aims to describe users' digital-health usage characteristics, assess their perceptions of behavioral-data utilization and digital-health trust, and examine the association between the two constructs. By doing so, the study provides a more nuanced understanding of how users interpret the expanding role of behavioral data in personalized digital health and offers an empirical basis for designing data-driven services that are not only personalized, but also perceived as trustworthy.

2. Theoretical Background and Literature Review

2.1. Data-Driven Digital Health

Digital health is increasingly evolving from a service-delivery model toward a data-driven environment in which user-generated information is collected, processed, and transformed into personalized services [14]. Digital-health platforms can use information generated through users' activities, interactions, health histories, and service engagement to provide recommendations, reminders, health information, and other tailored functions [2]. Consequently, the value of digital health increasingly depends not only on technological accessibility but also on how effectively platforms transform user data into relevant service outcomes.

This development creates a fundamental tension between personalization and information privacy [4]. Personalized services require access to user information, while users may simultaneously be concerned about how such information is collected and subsequently used. Information privacy concerns are fundamentally related to individuals' desire to control or influence the collection and use of information about themselves [7]. In digital health, this issue is particularly consequential because the information involved may include sensitive health and behavioral data.

The resulting environment requires users to evaluate not only the usefulness of digital-health services but also the trustworthiness of the platforms responsible for handling their data. This study addresses this issue by examining users' Perceived Behavioral Data Utilization (PBDU) and its association with Digital Health Trust (DHT).

2.2. Behavioral Data Utilization in Digital Health

Behavioral data utilization refers to users' perceptions that information generated through their activities and interactions with digital-health platforms is collected, processed, and subsequently used to support service delivery [15]. In this study, PBDU is conceptualized through three dimensions: data collection, data processing, and data

utilization. This structure represents a progressive data lifecycle in which information is captured, analyzed, and translated into service-related outcomes [16].

Data collection concerns users' recognition that platforms record their activities, interactions, and health-related information. Data processing concerns the perceived analysis of such information to understand users and their needs. Data utilization concerns the perceived application of processed information to improve services or provide personalized recommendations. Thus, PBDU extends beyond awareness that data are collected; it captures the perception that user data are actively transformed into service value [17], [18].

Personalization provides one of the most visible manifestations of such utilization. Awad and Krishnan [19] demonstrated the personalization–privacy paradox: firms require consumer information to provide personalized services, yet consumers who value information transparency may also be less willing to participate in profiling [4]. This tension is particularly relevant in health contexts because personalization may depend on information that is substantially more sensitive than ordinary consumer data.

The distinction between collection and utilization is therefore theoretically important. Users may readily recognize that a platform collects information without fully understanding how the information is subsequently processed. Conversely, personalized recommendations or reminders can make otherwise invisible data practices more observable. PBDU consequently captures users' perceptions of the broader data-use process rather than merely their awareness of data collection.

2.3. Trust in Data-Driven Digital Health

Trust provides the primary theoretical foundation for understanding how users evaluate digital-health platforms that handle personal information. Mayer et al [20] conceptualize trustworthiness through three characteristics of the trustee: ability, benevolence, and integrity. Ability concerns the perceived competence of the trustee; benevolence reflects the belief that the trustee intends to act in the trustor's interests; and integrity concerns adherence to acceptable principles and commitments.

This framework is highly relevant to digital-health platforms. Users need to believe that a platform is technically capable of managing their information, acts in ways that consider users' interests, and behaves consistently with its stated commitments concerning data protection and service provision. Accordingly, DHT in this study is represented through competence, benevolence, and integrity.

The importance of trust is particularly pronounced in digital health because users operate under uncertainty regarding technological processes and organizational data practices [21]. Adjekum et al [22], in a scoping review of 278 studies, identified privacy, usefulness, customizable design, interoperability, service-provider reputation, and fair

data access among the factors associated with trust in digital-health systems, while fear of data exploitation and defective technology were identified as impediments.

Thus, DHT should not be understood simply as a general favorable attitude toward digital health. It represents a multidimensional assessment of whether the platform is capable, appropriately motivated, and reliable in its handling of users and their information.

2.4. Privacy Calculus and Personal-Data Disclosure

Privacy Calculus Theory provides a complementary perspective for explaining why users may disclose personal information despite potential privacy risks [23]. The theory proposes that individuals evaluate anticipated benefits against perceived risks when deciding whether to disclose personal information. Dinev and Hart [24] found that although privacy concerns inhibit disclosure, trust and perceived benefits can outweigh privacy-risk perceptions in online transactions [13].

This perspective is especially relevant to digital health, where users may disclose sensitive information in exchange for perceived health-related benefits [3]. Bansal et al [25] specifically demonstrated the importance of trust, privacy concern, and information sensitivity in the disclosure of health information online. Their findings reinforce the view that health-information disclosure is not determined solely by the sensitivity of information but also by users' evaluation of the entity receiving and handling that information.

The privacy-calculus perspective also helps explain why data utilization does not necessarily generate distrust [23]. If users perceive that their information produces meaningful and relevant services, the perceived benefits of data use may coexist with concerns about privacy. In digital health, personalized reminders, recommendations, and health information can therefore represent perceived benefits that help justify continued engagement with data-driven platforms [2].

However, personalization does not eliminate the importance of transparency and responsible data governance. The personalization–privacy literature indicates that greater personalization can require greater access to personal information, creating an inherent tension between service value and privacy expectations [19]. Privacy calculus therefore provides an appropriate contextual lens for understanding the coexistence of data disclosure, personalization, and trust without assuming that users necessarily perceive data utilization as either wholly beneficial or wholly threatening [26].

2.5. Relationship Between Behavioral Data Utilization and Digital Health Trust

The relationship between PBDU and DHT can be theoretically understood by integrating trust theory with the privacy-calculus perspective [27]. Perceived behavioral-data utilization makes data practices more salient to users. Once users recognize that their information is collected, processed, and utilized, they can evaluate whether the platform

appears capable of managing those data, whether its use of data appears aligned with users' interests, and whether its practices are consistent with its commitments.

Importantly, greater perceived data utilization does not necessarily imply lower trust. Data utilization can simultaneously represent value creation and potential risk [28]. When users perceive that their data are transformed into useful and relevant services, utilization may provide evidence of platform competence. When such utilization appears to address users' needs, it may also be interpreted as evidence of benevolence. However, utilization alone does not establish integrity; users must still believe that the platform is honest, responsible, and consistent in its data practices [12].

Recent digital-health research supports the importance of this interaction. Liu and Tao [11] found that personalization and loss of privacy are important characteristics influencing acceptance of smart healthcare services, while trust plays a central role in translating these characteristics into acceptance. This suggests that personalization and privacy should not be examined independently from users' trust evaluations [4].

Building on these perspectives, this study proposes that users who perceive stronger behavioral-data utilization will tend to report stronger trust in digital-health platforms. Because the present study uses cross-sectional survey data and examines the relationship through correlation analysis, the proposition is formulated as an association rather than a causal effect.

H1: Perceived Behavioral Data Utilization is positively associated with Digital Health Trust.

2.6. Research Framework

The theoretical framework positions PBDU as the focal perception of data-driven platform practices and DHT as the focal evaluation of platform trustworthiness. PBDU encompasses data collection, data processing, and data utilization, whereas DHT encompasses integrity, benevolence, and competence. The framework is anchored primarily in multidimensional trust theory, while Privacy Calculus Theory provides a complementary explanation for the coexistence of personal-data disclosure, perceived benefits, privacy considerations, and trust [13].

The framework therefore moves beyond a simple assumption that increased use of personal data inevitably reduces trust. Instead, it proposes that users may simultaneously recognize substantial behavioral-data utilization and maintain trust when such utilization is perceived as competent, beneficial, and consistent with responsible platform behavior. The empirical analysis subsequently tests whether this theoretical expectation is reflected in the observed association between PBDU and DHT.

3. Methods

3.1. Research Design

This study employed a quantitative, cross-sectional survey design to describe digital-health platform usage and examine the association between PBDU and DHT. The study was primarily descriptive, with correlational analysis used to assess the relationship between the two focal constructs [29]. Because data were collected during a single survey period, the analysis was intended to identify patterns and associations rather than establish causal relationships.

3.2. Survey Instrument

The questionnaire covered respondent characteristics, platform usage, exposure to personalized digital-health services, data-disclosure practices, PBDU, and DHT. It began with introductory information explaining the study's purpose and an informed-consent statement, allowing respondents to proceed only after consenting.

The measurement items for PBDU and DHT were newly developed and adapted specifically for this study based on a theoretical synthesis of behavioral analytics and digital health trust frameworks. PBDU and DHT were each measured using nine items across three specific dimensions (data collection, processing, and utilization for PBDU; integrity, benevolence, and competence for DHT) [12] using a five-point Likert-type scale. The complete English-language version of the survey instrument is provided as Additional file 1. Categorical usage and disclosure questions were analyzed according to their specified response formats, treating single-choice items as mutually exclusive.

3.3. Data Collection

Conducted throughout August 2026, the questionnaire was distributed online via Google Forms for remote completion. This online approach was chosen to align with the focus on digital-health platform experiences. Participation was voluntary and preceded by introductory details and consent statements, adhering to basic transparency and procedure principles for internet-based surveys [30]. A total of 485 valid responses were analyzed to describe the sample rather than generalize to a broader population.

3.4. Data Processing and Statistical Analysis

Data processing and statistical analysis were conducted using Python in a Jupyter Notebook environment [31], [32]. The dataset obtained from Google Forms was imported into the Python environment and organized according to the variables and constructs specified in the questionnaire. The analytical workflow included data preparation, descriptive analysis, reliability assessment, correlation analysis, and visualization.

Pearson’s correlation coefficient (r) was then used to assess the direction and strength of the association between the two constructs. Correlation analysis was also extended to their respective dimensions to provide a more detailed assessment of the relationships between perceived behavioral-data utilization and digital-health trust.

The interpretation of Pearson's correlation was based on the coefficient's direction and magnitude, while statistical significance was evaluated using the corresponding *p*-value. Since the study employed a cross-sectional design, statistically significant correlations were interpreted as evidence of association rather than causation.

Python was also used to generate the visualizations presented in the Results and Discussion section. These included the comparison of mean scores across PBDU and DHT dimensions and the graphical representation of the association between the two focal constructs. The use of Jupyter Notebook enabled the data-processing procedures, statistical calculations, and graphical outputs to be maintained within a single computational workflow, supporting analytical transparency and reproducibility [33].

3.5. Ethical Considerations

Ethical considerations were incorporated into the online survey through the provision of introductory information and informed consent before participation. Participation was voluntary, and respondents were given the opportunity to decide whether to participate after receiving information about the study.

The analysis focused on aggregated survey responses, and the findings are reported at the group level rather than at the individual level. The survey procedure and reporting of the online data-collection process were guided by established recommendations for internet-based survey research [30].

4. Results and Discussion

This section presents the empirical findings on respondents' digital-health usage characteristics, PBDU, and DHT. The analysis first describes the respondents and their patterns of digital-health platform use, followed by descriptive and reliability statistics for the two focal constructs. The analysis then examines the association between PBDU and DHT and discusses the principal findings in relation to behavioral-data visibility, trust in data-driven digital health, and the implications of personalized digital-health services.

4.1. Respondent Characteristics

Table 1 presents the demographic characteristics of the 485 valid respondents included in the analysis. The sample is characterized by a relatively strong concentration in the male group, which accounts for 315 respondents (64.9%), while female respondents account for 170 (35.1%). This distribution indicates that the observed perceptions and usage patterns in the present study are derived from a sample in which male users constitute the majority. Accordingly, the findings should be interpreted as descriptive of the surveyed user group rather than as evidence of population-level gender differences.

Table 1. Respondent Characteristics

Characteristic	Category	n	%
Gender	Male	315	64.9
	Female	170	35.1
Age	18–24	3	0.6
	25–34	251	51.8
	35–44	212	43.7
	45–54	19	3.9
	≥55	0	0.0
Education	High school/equivalent	81	16.7
	Diploma	58	12.0
	Bachelor's	215	44.3
	Master's	126	26.0
	Doctoral	5	1.0

The age distribution is considerably more concentrated than the gender distribution. More than half of the respondents are aged 25–34 years (n = 251; 51.8%), followed by those aged 35–44 years (n = 212; 43.7%). Together, these two age groups represent 95.5% of the sample. Only 19 respondents (3.9%) are aged 45–54 years, while three respondents (0.6%) are aged 18–24 years. No respondent is represented in the 55-years-or-older category. The sample therefore predominantly represents adults in the 25–44 age range, suggesting that the subsequent findings primarily reflect the experiences of relatively mature digital-health users rather than those of the youngest or oldest user groups.

The educational profile further indicates that the sample is relatively highly educated. Respondents holding a bachelor's degree constitute the largest educational group (n = 215; 44.3%), followed by master's degree holders (n = 126; 26.0%). High school or equivalent graduates account for 81 respondents (16.7%), while 58 respondents (12.0%) hold a diploma and five (1.0%) hold a doctoral degree. Thus, 71.3% of respondents possess at least a bachelor's degree. This concentration is relevant when interpreting subsequent findings concerning behavioral-data utilization and trust because the sample largely consists of respondents with tertiary educational backgrounds.

Taken together, the respondent profile indicates that the empirical evidence is predominantly shaped by male users aged 25–44 years with relatively high levels of formal education. This profile provides an important context for interpreting the subsequent analysis. In particular, the strong representation of respondents within the 25–44 age range and the substantial proportion of university graduates indicate that the study captures digital-health experiences primarily among adult users who are already represented in formal digital-health interactions. However, the uneven distribution across demographic categories also means that the findings should not be generalized

indiscriminately to underrepresented groups, particularly users aged 18–24 and those aged 55 years or older.

4.2. Digital Health Platform Usage Characteristics

The respondents' digital-health usage characteristics provide an important behavioral context for interpreting their perceptions of behavioral-data utilization and trust. Rather than treating PBDU and DHT as isolated perceptions, the usage profile illustrates the extent to which respondents are already engaged with digital-health platforms, the purposes for which these platforms are accessed, the personalized services encountered, and the extent to which personal information is disclosed.

4.2.1. Duration and frequency of digital-health use

Table 2 shows that respondents are generally not long-term users of digital-health platforms. The largest group, comprising 261 respondents (53.8%), reported using digital-health platforms for 6–12 months. A further 164 respondents (33.8%) had used such platforms for 1–2 years. In contrast, only 28 respondents (5.8%) reported usage of less than six months, while 24 (4.9%) had used digital-health platforms for 2–5 years and only eight (1.6%) for more than five years. Thus, 87.6% of respondents had used digital-health platforms for between six months and two years. The sample therefore reflects substantial exposure to digital-health services, while relatively few respondents can be characterized as very recent or highly experienced long-term users.

Table 2. Duration and Frequency of Digital-Health Platform Use

Duration of use	**Duration**	**n**	**%**
	<6 months	28	5.8
	6–12 months	261	53.8
	1–2 years	164	33.8
	2–5 years	24	4.9
	>5 years	8	1.6
Frequency of use	**Frequency**	**n**	**%**
	Almost every day	6	1.2
	Several times/week	195	40.2
	Several times/month	235	48.5
	Several times/year	43	8.9
	Rarely	6	1.2

The frequency distribution reinforces this pattern. Almost half of the respondents (n = 235; 48.5%) reported using digital-health platforms several times per month, followed by 195 respondents (40.2%) who used them several times per week. Only six respondents (1.2%) reported almost-daily use, while 43 (8.9%) used the platforms several times per

year and six (1.2%) reported using them rarely. Overall, the findings indicate that digital-health engagement among the respondents is predominantly periodic rather than daily. This distinction is important because perceptions of how platforms collect and utilize behavioral data may develop through repeated interactions without requiring continuous daily use.

4.2.2. Patterns of digital-health utilization

Table 3 describes the respondents' primary utilization patterns and the devices used to access digital-health platforms. Reading health information is the most frequently reported primary use, selected by 189 respondents (39.0%). Hospital appointment booking follows with 96 respondents (19.8%), while health monitoring accounts for 79 (16.3%). Laboratory testing is the primary purpose for 49 respondents (10.1%), followed by online medical consultation with 42 (8.7%) and purchasing medicines with 24 (4.9%). Insurance claims represent only five respondents (1.0%), while one respondent (0.2%) reported another purpose related to the COVID-19 period.

Table 3. Patterns of Digital-Health Platform Utilization

Primary purpose of use	**Descriptin**	**n**	**%**
	Online medical consultation	42	8,7%
	Purchasing medicines	24	4,9%
	Laboratory tests	49	10,1%
	Reading health information	189	39,0%
	Hospital appointment booking	96	19,8%
	Health monitoring	79	16,3%
	Insurance claims	5	1,0%
	Others: During Covid-19	1	0,2%
Primary access device	**Descriptin**	**n**	**%**
	Smartphone	332	68,5%
	Tablet	95	19,6%
	Laptop	53	10,9%
	Desktop Computer	5	1,0%

This distribution suggests that respondents' engagement with digital health is oriented strongly toward information access and service coordination rather than exclusively toward direct clinical interaction. The prominence of health-information seeking is particularly notable because such interactions may expose users to personalized content and recommendation mechanisms even when users are not directly seeking a consultation [34].

The device profile is even more concentrated. Smartphones are the dominant access device, reported by 332 respondents (68.5%), followed by tablets (95; 19.6%) and laptops (53; 10.9%). Desktop computers account for only five respondents (1.0%). The

overwhelming predominance of mobile access indicates that respondents' digital-health interactions occur mainly through personal, portable devices. This pattern provides a relevant behavioral context for subsequent findings concerning data utilization and personalization because repeated platform interactions through mobile devices can involve diverse forms of user activity and service engagement [3].

4.2.3. Exposure to personalized digital-health services

Table 4 presents the types of personalized digital-health services reportedly received by respondents. Appointment reminders constitute the most prevalent form of personalization, reported by 179 respondents (36.9%). Personalized health articles are the second most common category (n = 110; 22.7%), followed by medication reminders (n = 64; 13.2%) and medication recommendations (n = 46; 9.5%). Doctor recommendations were reported by 34 respondents (7.0%), while personalized promotional offers and health-screening recommendations were each reported by 25 respondents (5.2%). Only two respondents (0.4%) reported other forms of personalized service.

Table 4. Exposure to Personalized Digital-Health Services

Personalized service	**n**	**%**
Doctor recommendations	34	7.0
Medication recommendations	46	9.5
Medication reminders	64	13.2
Appointment reminders	179	36.9
Personalized health articles	110	22.7
Personalized promotional offers	25	5.2
Health screening recommendations	25	5.2
Other	2	0.4

The distribution indicates that personalization is experienced predominantly through reminder and information-oriented functions. This is analytically relevant to PBDU because these services can make the utilization of user-related information visible through concrete outputs, even when users may not directly observe the underlying data-processing processes. In other words, personalization provides an observable interface between data use and the service experience. The findings therefore establish an important empirical context for examining whether respondents perceive that their behavioral data are being collected, processed, and utilized to support more tailored digital-health services.

4.2.4. Personal-data disclosure

Table 5 summarizes both the frequency with which respondents provide personal information and the types of information disclosed. Personal-data disclosure is relatively

common within the surveyed group. Nearly half of the respondents (n = 230; 47.4%) reported that they often provide personal information to digital-health platforms, while 172 (35.5%) do so sometimes. A further 37 respondents (7.6%) reported always providing personal information, compared with 44 (9.1%) who do so rarely and only two (0.4%) who never do so. Hence, 90.5% of respondents reported providing personal information at least sometimes.

Table 5. Personal-Data Disclosure Practices Among Respondents

Frequency of personal-data disclosure	**Frequency**	**n**	**%**
	Always	37	7.6
	Often	230	47.4
	Sometimes	172	35.5
	Rarely	44	9.1
	Never	2	0.4
Types of personal data disclosed	**Data type**	**n**	**%**
	Consultation history	120	24.7
	Medical history	108	22.3
	Medication purchase history	81	16.7
	Name/personal identification	70	14.4
	Medical test results	45	9.3
	Email	22	4.5
	Lifestyle information	20	4.1
	Phone number	7	1.4
	Location	6	1.2
	Photograph	6	1.2

The types of disclosed information indicate that disclosure extends beyond basic identification data. Consultation history is the most frequently reported category (n = 120; 24.7%), followed by medical history (n = 108; 22.3%) and medication purchase history (n = 81; 16.7%). Name or personal identification information accounts for 70 respondents (14.4%), while medical test results account for 45 (9.3%). Less frequently reported categories include email addresses (22; 4.5%), lifestyle information such as exercise and sleep habits (20; 4.1%), telephone numbers (7; 1.4%), location (6; 1.2%), and photographs (6; 1.2%).

Taken together, these findings show that respondents' digital-health engagement involves not only routine service use but also meaningful disclosure of health-related and interaction-related information. The prominence of consultation history, medical history, and medication purchase history is particularly important because these forms of information can provide platforms with a richer representation of users' health-related

behaviors and interactions. The observed combination of frequent personal-data disclosure and exposure to personalized services therefore provides a strong empirical foundation for the subsequent analysis of perceived behavioral-data utilization and digital health trust [12].

4.3. Descriptive Statistics and Reliability of the Constructs

Table 6 summarizes the descriptive statistics and internal consistency of the two focal constructs, Perceived Behavioral Data Utilization (PBDU) and Digital Health Trust (DHT). Across all 18 measurement items, the median is consistently 4, indicating that the central response for both constructs is positioned toward the upper end of the five-point response scale. The item-level means also show a generally favorable pattern, with PBDU means ranging from 3.934 to 4.113 and DHT means ranging from 3.899 to 4.027. These results indicate that respondents generally perceived relatively substantial utilization of behavioral data and reported relatively high levels of trust in digital-health platforms.

Table 6. Descriptive Statistics and Reliability of the PBDU and DHT Constructs

Construct/Item	Mean	SD	Median	Min–Max	Cronbach's α
PBDU					
PBDU1	4.113	0.690	4	2–5	0.897
PBDU2	4.087	0.702	4	2–5	
PBDU3	4.035	0.725	4	2–5	
PBDU4	4.070	0.732	4	2–5	
PBDU5	4.056	0.743	4	2–5	
PBDU6	3.934	0.782	4	2–5	
PBDU7	4.021	0.766	4	2–5	
PBDU8	3.940	0.682	4	2–5	
PBDU9	4.062	0.572	4	2–5	
DHT					
DHT1	3.957	0.787	4	2–5	0.909
DHT2	4.027	0.764	4	1-5	
DHT3	3.957	0.763	4	2-5	
DHT4	3.992	0.785	4	2-5	
DHT5	3.936	0.791	4	2-5	
DHT6	3.899	0.818	4	1-5	
DHT7	4.006	0.834	4	1-5	
DHT8	3.930	0.727	4	2-5	
DHT9	4.004	0.692	4	2–5	

4.3.1. Perceived Behavioral Data Utilization (PBDU)

The PBDU results indicate a consistently positive perception of behavioral-data utilization across the nine measurement items. As illustrated in Figure 1(a), the mean scores are relatively high and closely distributed across the three dimensions of data collection, data processing, and data utilization, indicating that respondents generally perceived behavioral-data use as an integrated component of their digital-health experience rather than as an isolated activity. The highest mean is observed for PBDU1 (M = 4.113, SD = 0.690), concerning the perception that digital-health platforms collect users' activity data. This is followed by PBDU2 (M = 4.087, SD = 0.702), which concerns the recording of users' interaction histories. These results indicate that the collection and recording of behavioral information constitute the most visible aspects of data utilization from the users' perspective.

The remaining items also demonstrate comparatively high mean scores. PBDU4, concerning the analysis of user data to understand health needs, records a mean of 4.070, while PBDU9, concerning the perceived use of provided data to improve service quality, records a mean of 4.062. By contrast, PBDU6 (M = 3.934) and PBDU8 (M = 3.940) produce the lowest mean scores within the construct. As reflected in Figure 1(a), however, the differences between the item means are relatively limited. This pattern suggests that respondents' perceptions remain broadly consistent across the data lifecycle, from collection and processing to service utilization.

The relatively high scores across all three dimensions are noteworthy because they indicate that respondents perceive behavioral-data utilization not merely as a background technical process but as a meaningful component of digital-health service delivery [3]. In particular, the comparatively strong scores for data collection and interaction recording suggest that users are more readily aware of the initial stages of data utilization, whereas the slightly lower scores for analytical processing and personalized use may indicate that downstream data practices are less directly observable.

The reliability result further supports the internal consistency of the construct. PBDU produces a Cronbach's alpha of 0.897, indicating high internal consistency among its nine measurement items. Overall, the descriptive evidence and the dimensional pattern shown in Figure 1(a) suggest that behavioral-data utilization is relatively salient in respondents' perceptions of digital-health platforms, providing an important empirical foundation for examining its relationship with trust.

4.3.2. Digital Health Trust (DHT)

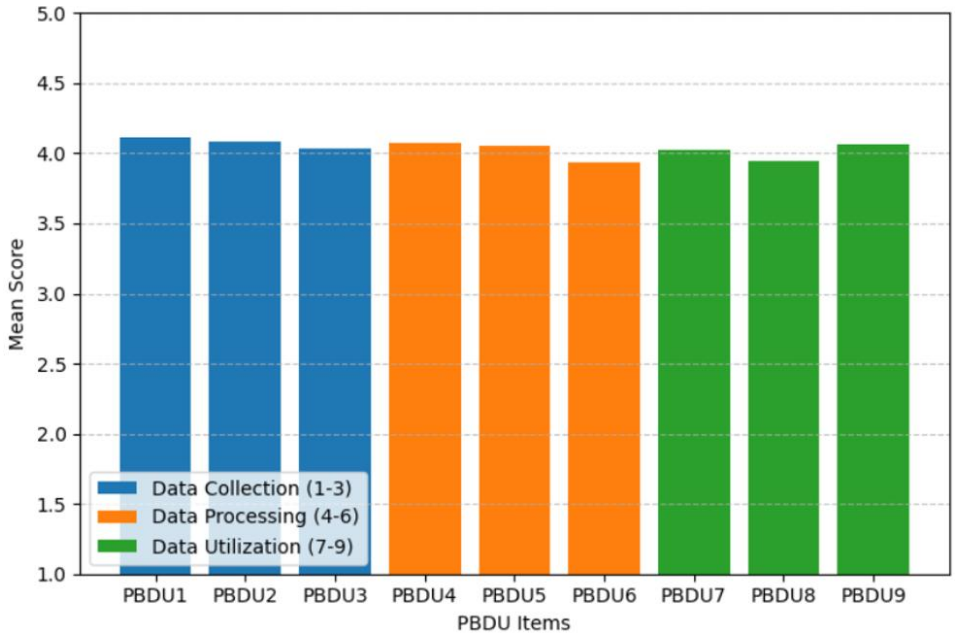
DHT also demonstrates a consistently favorable response pattern across its nine measurement items. Figure 1(b) illustrates that the mean scores across the three trust dimensions (integrity, benevolence, and competence) remain relatively close to one another, indicating that respondents' trust is not concentrated exclusively in a single

dimension. The highest mean is observed for DHT2 (M = 4.027, SD = 0.764), reflecting respondents' confidence that platforms fulfill their commitments to protecting user data. This is followed by DHT7 (M = 4.006, SD = 0.834) and DHT9 (M = 4.004, SD = 0.692), which concern the platform's ability to manage user data and the adequacy of its technology for maintaining data security, respectively.

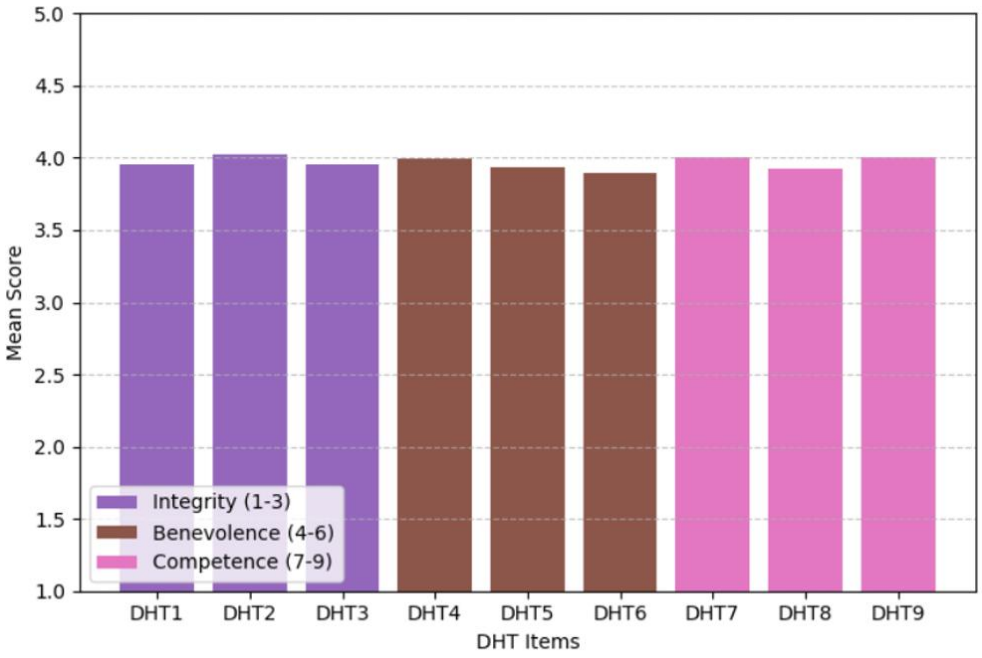
These results indicate that perceptions of data protection and technical competence constitute particularly strong elements of trust in the surveyed digital-health context. At the same time, the lowest mean is observed for DHT6 (M = 3.899, SD = 0.818), concerning the belief that the platform will not intentionally harm its users. DHT5 (M = 3.936) and DHT8 (M = 3.930) also show comparatively lower mean scores, although all remain close to 4 on the five-point scale. The relatively narrow distribution of scores, also visible in Figure 1(b), suggests that respondents evaluate trust through a combination of platform integrity, benevolent orientation, and technological competence rather than through a single dominant attribute.

The Cronbach's alpha of 0.909 demonstrates high internal consistency across the nine DHT items. Taken together, the descriptive pattern indicates that respondents generally express favorable trust toward data-driven digital-health platforms, particularly regarding their ability to protect and manage user data. However, the findings also suggest that trust involves more than technical security. Confidence that a platform acts in the user's interest and avoids harmful behavior remains an important component of the overall trust construct.

The combination of relatively high PBDU and DHT scores provides an important basis for the subsequent association analysis. Rather than suggesting that greater perceived use of behavioral data is inherently incompatible with trust, the descriptive findings indicate that users may simultaneously recognize data utilization and maintain confidence in the platform.



(a) PBDU



(b) DHT

Figure 1. Mean Scores Across Dimensions

4.4. Association Between PBDU and DHT

Table 7 and Figure 2 examine the association between Perceived Behavioral Data Utilization (PBDU) and Digital Health Trust (DHT). The Pearson correlation analysis produces a correlation coefficient of $r = 0.440$, with $p = 2.4758 \times 10^{-24}$. The result indicates a positive and statistically significant association between the two constructs.

In substantive terms, respondents who reported stronger perceptions that digital-health platforms collect, process, and utilize behavioral data also tended to report higher levels of trust in those platforms.

Table 7. Pearson Correlations Between PBDU, DHT, and Their Dimensions

	PBDU	**PBDU Collection**	**PBDU Processing**	**PBDU Utilization**
DHT	**0.440**			
DHT Integrity		0.273	0.279	0.289
DHT Benevolence		0.380	0.415	0.404
DHT Competence		0.380	0.406	**0.444**

The magnitude of the coefficient indicates a moderate positive association rather than an extremely strong relationship. This distinction is important. The result demonstrates that PBDU and DHT move in the same direction within the observed sample, but PBDU does not fully account for variation in trust. Trust in digital-health platforms therefore appears to encompass considerations beyond perceived behavioral-data utilization alone.

The dimension-level correlations provide a more differentiated picture. As shown in Table 7, the three PBDU dimensions (data collection, data processing, and data utilization) are positively correlated with all three DHT dimensions: integrity, benevolence, and competence. The correlations with DHT integrity range from 0.273 to 0.289, indicating relatively modest positive associations. Stronger relationships are observed for DHT benevolence, with coefficients ranging from 0.380 to 0.415, and for DHT competence, with coefficients ranging from 0.380 to 0.444. The strongest dimension-level association is between PBDU utilization and DHT competence ($r = 0.444$).

This pattern is analytically important because it suggests that the perceived use of behavioral data is more closely aligned with perceptions of platform competence and benevolence than with integrity. Respondents may therefore interpret visible data-driven functionality not merely as evidence that a platform possesses data, but also as an indication of its capability to transform data into useful and personalized services [35], [36]. At the same time, the weaker correlations with integrity indicate that recognizing data utilization does not necessarily translate into equally strong perceptions that the platform is honest or consistently adheres to its stated privacy commitments.

Figure 2 visually reinforces the positive direction of the overall association. Nevertheless, the correlational nature of the analysis requires a cautious interpretation. The findings establish an association between PBDU and DHT, but they do not demonstrate that perceived behavioral-data utilization causes greater trust. Rather, they indicate that the two perceptions are empirically connected within the surveyed population. This finding provides the basis for the subsequent discussion of behavioral-data visibility, trust

formation, and the implications of data-driven personalization in digital-health environments.

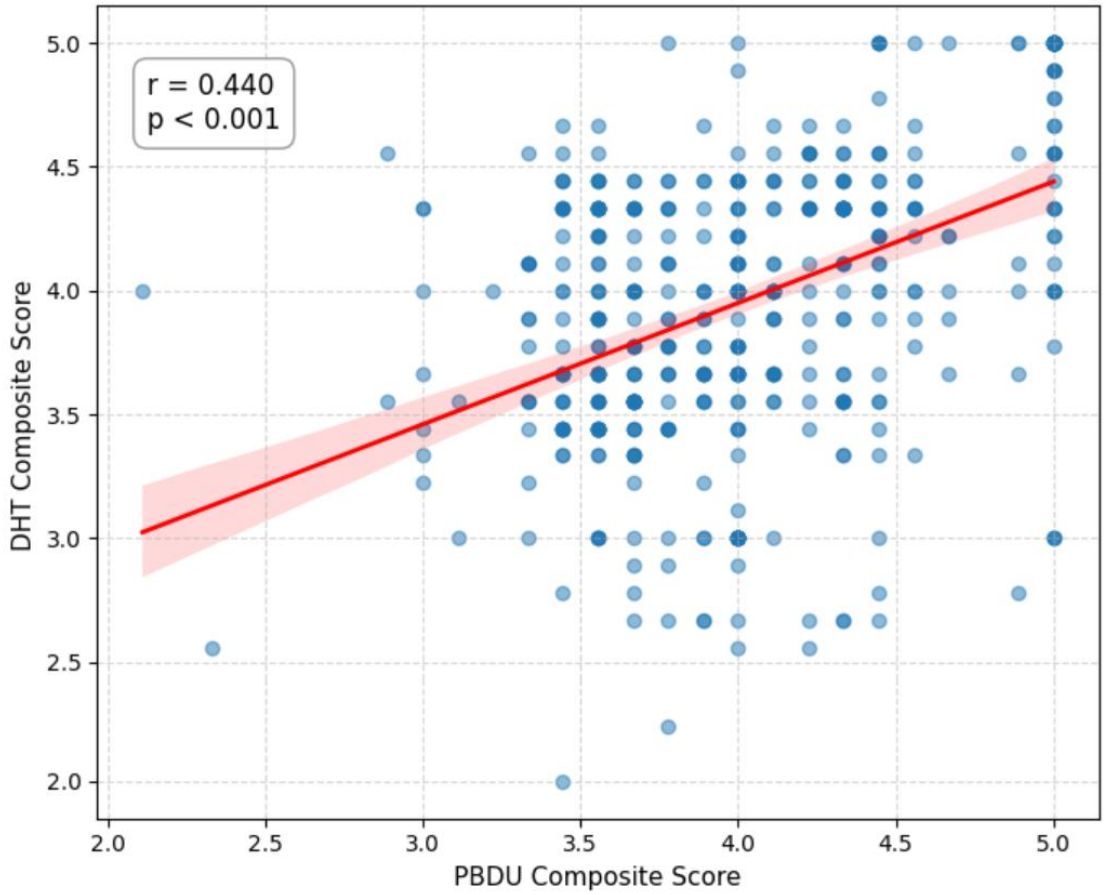


Figure 2. Association Between PBDU and DHT

4.5. Discussion of Key Findings

The findings provide a coherent picture of how users experience data-driven digital health. The respondents are predominantly adults aged 25–44 years, most have tertiary education, and the majority use digital-health platforms several times per month or week. Their engagement is concentrated around health-information access, appointment-related services, and health monitoring, while smartphones represent the dominant access device. More importantly, most respondents report providing personal information at least sometimes, with consultation history, medical history, and medication purchase history among the most frequently disclosed data types. Against this behavioral background, respondents report relatively high perceptions of behavioral-data utilization and digital health trust [3], while the two constructs demonstrate a moderate positive association.

4.5.1. Visibility of Behavioral Data Utilization

A central finding is that behavioral-data utilization appears to be relatively visible to users, particularly at the stages of data collection and interaction recording. PBDU1 and PBDU2 obtain the two highest mean scores within the construct, suggesting that respondents are more readily aware that platforms collect activity data and record interaction histories. This visibility becomes somewhat less pronounced when the process moves from collection toward analytical utilization, as reflected in the comparatively lower scores for PBDU6 and PBDU8.

This pattern is significant because behavioral-data utilization is inherently a multi-stage process. Users may observe the immediate consequences of providing information or interacting with a platform without directly observing how those data are subsequently processed. The results suggest that respondents nevertheless possess a relatively strong perception that such processing and utilization occur. The distinction between visible collection and less visible analytical use therefore represents an important characteristic of the digital-health experience.

The high overall PBDU scores should not be interpreted as evidence that respondents possess detailed technical knowledge of platform data practices. Rather, they indicate a perception that user-related data are being collected, processed, and used in connection with digital-health services. This distinction is particularly relevant in the context of personalization. The findings on personalized services show that appointment reminders and personalized health articles are prominent forms of personalization [37]. Such outputs can make underlying data utilization more tangible because users can directly observe a service that appears responsive to their information or prior interactions.

4.5.2. Trust in Data-Driven Digital Health

The second major finding is the generally favorable level of trust reported by respondents. All nine DHT items have medians of 4, and the item means remain close to 4. The strongest response concerns confidence that platforms honor their commitments to protect user data (DHT2, M = 4.027). High scores are also observed for platform capability in managing user data (DHT7, M = 4.006) and technological adequacy for data security (DHT9, M = 4.004).

These results indicate that trust is associated not only with perceived privacy protection but also with perceptions of technical capability. Conversely, DHT6, concerning whether platforms would intentionally harm users, has the lowest mean (M = 3.899). Although the difference is relatively small, it suggests that confidence in the platform's technical and protective capabilities may be somewhat more pronounced than confidence concerning its broader benevolent orientation [38].

The three dimensions of DHT (integrity, benevolence, and competence) therefore appear to operate as complementary components of trust. Users' trust cannot be reduced to data security alone. A trusted digital-health platform is perceived as one that protects data, manages data competently, provides reliable services, and acts in ways that users perceive as consistent with their interests. The high Cronbach's alpha for DHT (0.909) further indicates that these dimensions are represented by a highly consistent set of measurement items.

4.5.3. The PBDU–Trust Relationship

The most consequential empirical finding is the positive association between PBDU and DHT ($r = 0.440$, $p < 0.001$). The result indicates that stronger perceptions of behavioral-data utilization tend to coexist with stronger trust in digital-health platforms. This finding challenges an overly simplistic assumption that greater awareness of data utilization necessarily produces distrust.

Instead, the evidence points toward a more nuanced interpretation: data utilization may be compatible with trust when users perceive that the data are translated into meaningful, reliable, and personalized services. The dimension-level results reinforce this interpretation. PBDU utilization has its strongest association with DHT competence ($r = 0.444$), while the PBDU dimensions generally show stronger correlations with benevolence and competence than with integrity.

The pattern suggests that users may evaluate data-driven digital health partly through the outcomes and capabilities that become visible through platform use. When data utilization is perceived as supporting useful recommendations, reminders, information, or other personalized functions, it may coexist with confidence in the platform's competence and consideration for users [11]. However, the comparatively weaker relationship with integrity is equally important. Perceiving that data are used does not automatically establish that a platform is perceived as honest, transparent, or consistently compliant with its privacy commitments [8].

Accordingly, the observed PBDU–DHT relationship should be interpreted as an association rather than a causal mechanism. The cross-sectional descriptive evidence cannot establish whether data utilization increases trust, whether trusted platforms encourage users to perceive data utilization more positively, or whether both perceptions are influenced by other factors. Nevertheless, the moderate positive correlation provides empirical evidence that perceived data utilization and trust are not inherently contradictory constructs within this sample.

4.5.4. Implications for Personalized Digital Health

The findings have several implications for the development of personalized digital-health services. First, personalization should not be treated solely as a technical capability.

Users appear to recognize data-driven functionality through visible service outcomes, particularly reminders and personalized health information [2]. Consequently, the value of personalization depends partly on whether users can understand the connection between their data and the services they receive [39].

Second, the results suggest that effective personalization should be accompanied by credible data practices. The relatively high PBDU scores indicate that respondents recognize that their behavioral and health-related information is being utilized, while the positive PBDU–DHT association indicates that such utilization can coexist with trust. This creates an important design principle: data-driven personalization should make the value of data use sufficiently visible [40] while maintaining confidence in the platform's competence, benevolence, and integrity [41].

Third, the findings highlight the importance of moving beyond a narrow privacy-versus-personalization framing. The data suggest that users do not necessarily perceive data utilization and trust as opposing conditions. Instead, trust may coexist with data utilization when users perceive the platform as capable of converting personal information into useful services. However, the weaker association between PBDU and integrity indicates that usefulness alone should not substitute for transparent and credible data governance.

Finally, the findings support a user-centered perspective on personalized digital health. Platforms should consider not only what data can technically be collected or processed, but also how users perceive the visibility, purpose, and value of that utilization. Personalized services should therefore be designed around a coherent relationship between data practices and user value: users provide information, the platform uses it responsibly, and the resulting personalization is sufficiently meaningful to justify continued engagement [40]. Within the limits of the present descriptive and correlational analysis, this perspective offers a useful basis for understanding why perceived behavioral-data utilization and trust can develop together in data-driven digital-health environments.

5. Conclusions

This study examined how users perceive behavioral-data utilization in digital-health platforms and how these perceptions are associated with trust in data-driven digital-health services. By combining descriptive evidence on digital-health usage with construct-level analysis of PBDU and DHT, the study provides an empirical view of how users interpret the growing role of personal and behavioral data in contemporary digital-health environments.

The findings indicate that respondents generally perceived behavioral-data utilization positively and consistently across the nine PBDU items. The strongest perceptions were associated with the collection of users' activity data and the recording of interaction

histories, suggesting that data collection represents one of the most visible aspects of data-driven digital-health services. Perceptions concerning the analysis of user information to understand health needs and the use of data to improve service quality were also relatively high. Although some PBDU items received comparatively lower mean scores, the differences were modest. This pattern suggests that respondents generally recognized behavioral-data utilization as a process extending beyond data collection to include subsequent processing and service-oriented use.

The results also demonstrate a favorable pattern of trust in digital-health platforms. Across the nine DHT items, respondents reported relatively high levels of trust, with particularly favorable perceptions concerning the platform's commitment to protecting user data, its ability to manage data, and the adequacy of its technological capabilities. The relatively narrow range of item means further indicates that trust was not concentrated on a single aspect of platform behavior. Rather, respondents appeared to evaluate digital-health platforms across multiple dimensions of trustworthiness, including competence, benevolence, and integrity.

The reliability analysis provides additional support for the measurement of the two focal constructs. PBDU demonstrated high internal consistency, with a Cronbach's alpha of 0.897, while DHT produced a Cronbach's alpha of 0.909. These results indicate that the items within each construct showed strong internal consistency and provide a sound basis for interpreting the subsequent construct-level analysis.

Most importantly, the analysis identified a positive association between PBDU and DHT ($r = 0.440$). This finding supports the proposed expectation that stronger perceptions of behavioral-data utilization tend to coexist with stronger trust in digital-health platforms. The result is theoretically meaningful because it challenges an overly simplistic assumption that greater awareness of data collection and utilization necessarily undermines trust. Instead, respondents may perceive data utilization as part of the value-generating capability of digital-health platforms, particularly when data are perceived to support useful, personalized, and relevant services.

The findings therefore suggest that trust in data-driven digital health should not be considered independently from users' perceptions of how their behavioral data are utilized. Data collection, processing, and utilization form an increasingly visible component of the digital-health experience, while trust provides an important interpretive mechanism through which users evaluate these practices. For digital-health providers, the implication is that responsible data utilization should extend beyond technical data management to include practices that are understandable, credible, and aligned with users' expectations.

From a theoretical perspective, the study contributes by bringing together perceived behavioral-data utilization and multidimensional digital-health trust within a single

empirical framework. Rather than treating data utilization exclusively as a privacy risk, the findings indicate that users can simultaneously perceive substantial data utilization and report relatively high trust. This provides a more nuanced perspective on the relationship between personalization, data practices, and trust in digital health.

Overall, the study demonstrates that users' perceptions of behavioral-data utilization are positively associated with their trust in digital-health platforms. However, given the cross-sectional and correlational nature of the study, this relationship should be interpreted as an observed association rather than evidence of causality. Future research should therefore examine the mechanisms through which data utilization perceptions may influence trust and determine whether the observed relationship remains stable across different populations, platforms, and digital-health contexts.

6. Limitations and Further Research

Several limitations should be considered when interpreting the findings of this study. First, the research employed a cross-sectional survey design. The design provides a snapshot of respondents' perceptions at a particular period and therefore does not permit conclusions about changes in perceptions over time or causal relationships between Perceived Behavioral Data Utilization and Digital Health Trust. The positive association identified in the analysis should consequently be interpreted as correlational evidence.

Second, the study relied on self-reported survey responses. Respondents reported their own perceptions of digital-health platform use, behavioral-data utilization, and trust. Such measures capture users' subjective interpretations rather than independently verified records of actual platform data practices. A respondent may perceive that a platform collects or utilizes behavioral data without having direct knowledge of the underlying technical processes. Future research could therefore combine survey responses with objective information about platform data practices, privacy policies, or observed system behavior.

Third, the online survey was administered through Google Forms and distributed electronically. Although this approach was appropriate for reaching users within a digitally mediated research context, online recruitment may introduce self-selection effects. Individuals who are more familiar with digital technologies or more engaged with digital-health services may be more likely to participate. Accordingly, the findings should not automatically be generalized to the broader population of digital-health users.

Fourth, the analytical model focused specifically on the association between PBDU and DHT. Other factors that may influence trust in digital-health platforms, such as privacy concerns, perceived risk, perceived benefits, transparency, perceived fairness, platform reputation, or prior experience, were not included as empirical variables in the present

study. Future research could incorporate these factors to develop a more comprehensive explanation of trust formation.

Further research could also employ longitudinal or experimental designs to investigate whether changes in perceived data utilization lead to changes in trust over time. Comparative studies across different digital-health platforms, demographic groups, or national contexts would provide additional evidence concerning the robustness and generalizability of the findings. Finally, future studies could extend the current framework by examining whether trust mediates the relationship between data utilization and outcomes such as continued platform use, willingness to disclose personal information, acceptance of personalized services, or user engagement. Such extensions would move beyond the descriptive and correlational scope of the present study toward a more comprehensive explanation of trust and data-related behavior in digital health.

Statements and Declarations

Authors' contributions

Faisal Binsar: Conceptualization, Methodology, Formal analysis, Investigation, Writing – original draft, Visualization, Supervision.
Erwin Tenggono: Methodology, Resources, Validation, Supervision, Writing – review & editing.
Dewi Sri Surya Wuisan: Investigation, Validation, Writing – review & editing.
All authors read and approved the final manuscript.

Funding

The authors received no external funding for this study.

Ethics approval and consent to participate

This study was approved by the Research Ethics Committee of Bina Nusantara University in accordance with the guidelines and regulations set forth by the institution and national standards. Informed consent was obtained from all participants prior to data collection.

Conflicts of Interest

The authors declare that they have no competing interests.

Data Availability Statement

The dataset generated and analyzed during the current study is not publicly available because it contains participant-level survey responses and may contain information that could potentially compromise participant confidentiality. Aggregated data supporting the findings of this study are available from the corresponding author upon reasonable request, subject to applicable ethical and privacy considerations.

Consent to Participate

All participants were provided with information about the purpose and procedures of the study before completing the online questionnaire. Participation was voluntary, and informed consent was obtained from participants prior to their participation in the study.

Consent for Publication

Not applicable. This study does not report any individually identifiable personal data or information that could identify individual participants.

AI Declaration

AI tools were used solely to support language refinement, paraphrasing, and minor editorial improvements. They were not used for data analysis, statistical computation, interpretation of results, or generation of the study's original scientific contributions. All AI-assisted content was critically reviewed and verified by the authors, who take full responsibility for the accuracy, integrity, and originality of the manuscript.

References

[1] C. Yang, Y. Chen, C. Qian, F. Shi, and Y. Guo, “The data-intensive research paradigm: challenges and responses in clinical professional graduate education,” *Front. Med.*, vol. 12, p. 1461863, 2025, doi: 10.3389/fmed.2025.1461863.

[2] I. Kassam, D. Ilkina, J. Kemp, H. Roble, A. Carter-Langford, and N. Shen, “Patient Perspectives and Preferences for Consent in the Digital Health Context: State-of-the-art Literature Review,” *J Med Internet Res*, vol. 25, p. e42507, 2023, doi: 10.2196/42507.

[3] J. Busch-Casler and M. Radic, “Trust and Health Information Exchanges: Qualitative Analysis of the Intent to Share Personal Health Information,” *J Med Internet Res*, vol. 25, p. e41635, 2023, doi: 10.2196/41635.

[4] F. Binsar, M. Hamsal, S. B. Abdinagoro, and M. Ichsan, “Navigating tensions in telemedicine: A dynamic equilibrium approach to challenges and opportunities in digital health,” *Telemat. Informatics Reports*, vol. 22, p. 100335, 2026, doi: https://doi.org/10.1016/j.teler.2026.100335.

[5] M. Rosenlund, U.-M. Kinnunen, and K. Saranto, “The Use of Digital Health Services Among Patients and Citizens Living at Home: Scoping Review,” *J. Med. Internet Res.*, vol. 25, p. e44711, Mar. 2023, doi: 10.2196/44711.

[6] D. Xu, M. Indulska, I. Asadi Someh, and G. Shanks, “Time to reassess data value: The many faces of data in organizations,” *J. Strateg. Inf. Syst.*, vol. 33, no. 4, p. 101863, 2024, doi: https://doi.org/10.1016/j.jsis.2024.101863.

[7] F. Bélanger and R. E. Crossler, “Privacy in the Digital Age: a Review of Information Privacy Research in Information Systems,” *Manag. Inf. Syst. Q.*, vol. 35, no. 4, pp. 1017-A36, Dec. 2011, doi: 10.2307/41409971.

[8] R. Gupta *et al.*, “Consumer Views on Privacy Protections and Sharing of Personal Digital Health Information,” *JAMA Netw. Open*, vol. 6, no. 3, pp. e231305–e231305, Mar. 2023, doi: 10.1001/jamanetworkopen.2023.1305.

[9] U. U. Mohd Hanafi, Z. R. Abu Hasan, N. F. Mokhtar, and P. N. Alagappar, “Digital natives’ privacy concerns in eHealth platforms,” *Digit. Transform. Soc.*, vol. 5, no. 2, pp. 200–216, Oct. 2025, doi: 10.1108/DTS-03-2025-0048.

[10] L. Nurgalieva and G. Doherty, “Privacy and security in digital therapeutics,” in *Digital Therapeutics for Mental Health and Addiction*, N. Jacobson, T. Kowatsch, and L. B. T.-D. T. for M. H. and A. Marsch, Eds., Academic Press, 2023, pp. 189–204. doi: https://doi.org/10.1016/B978-0-323-90045-4.00002-2.

[11] K. Liu and D. Tao, “The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services,” *Comput. Human Behav.*, vol. 127, p. 107026, 2022, doi: https://doi.org/10.1016/j.chb.2021.107026.

[12] A. Venkatasubramanian, “A digital health trust framework guided by values from the science of yoga,” *Oxford Open Digit. Heal.*, vol. 1, p. oqad007, Jan. 2023, doi: 10.1093/oodh/oqad007.

[13] B. Binzer, J. Kendziorra, A.-K. Witte, and T. J. Winkler, “Trust in Public and Private Providers of Health Apps and Usage Intentions ,” Jun. 2024. doi: 10.1007/s12599-024-00869-4 .

[14] N. Shapoo, N. Shapoo, A. Rehman, and N. Boma, “Smart Healthcare: The Role of Digital Health in Modern Medicine,” *Heal. care Sci.*, vol. 4, no. 3, pp. 179–187, Jun. 2025, doi: 10.1002/hcs2.70019.

[15] C. Lim, M. J. Kim, K. H. Kim, K. J. Kim, and P. P. Maglio, “Using data to advance service: managerial issues and theoretical implications from action research,” *J. Serv. Theory Pract.*, vol. 28, no. 1, pp. 99–128, 2018, doi: 10.1108/JSTP-08-2016-0141.

[16] R. D. Zielstorff, “Capturing and using clinical outcome data: implications for

information systems design," *J. Am. Med. Inform. Assoc.*, vol. 2, no. 3, pp. 191–196, 1995, doi: 10.1136/jamia.1995.95338872.

[17] J. Simonsson and G. Agarwal, "Perception of value delivered in digital servitization," *Ind. Mark. Manag.*, vol. 99, pp. 167–174, 2021, doi: https://doi.org/10.1016/j.indmarman.2021.10.011.

[18] Markus Blut, Damien Chaney, Renaud Lunardo, Rémi Mencarelli, and Dhruv Grewal, "Customer Perceived Value: A Comprehensive Meta-analysis," *J. Serv. Res.*, vol. 27, no. 4, pp. 501–524, Nov. 2024, doi: 10.1177/10946705231222295.

[19] N. F. Awad and M. S. Krishnan, "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *Manag. Inf. Syst. Q.*, vol. 30, no. 1, pp. 13–28, Mar. 2006, doi: 10.2307/25148715.

[20] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An Integrative Model Of Organizational Trust," *Acad. Manag. Rev.*, vol. 20, no. 3, pp. 709–734, Jul. 1995, doi: 10.5465/amr.1995.9508080335.

[21] B. K. Myskja and K. S. Steinsbekk, "Personalized medicine, digital technology and trust: a Kantian account," *Med. Heal. Care Philos.*, vol. 23, no. 4, pp. 577–587, 2020, doi: 10.1007/s11019-020-09974-z.

[22] A. Adjekum, A. Blasimme, and E. Vayena, "Elements of Trust in Digital Health Systems: Scoping Review," *J Med Internet Res*, vol. 20, no. 12, p. e11254, 2018, doi: 10.2196/11254.

[23] S. Li *et al.*, "Research on user's highly sensitive privacy disclosure intention in home intelligent health service system: A perspective from trust enhancement mechanism," *Digit. Heal.*, vol. 9, p. 20552076231219444, 2023, doi: 10.1177/20552076231219444.

[24] T. Dinev and P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, Mar. 2006, doi: 10.1287/isre.1060.0080.

[25] G. Bansal, F. "Mariam" Zahedi, and D. Gefen, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decis. Support Syst.*, vol. 49, no. 2, 2010, doi: 10.1016/j.dss.2010.01.010.

[26] A. N. Slepchuk, G. R. Milne, and K. Swani, "Overcoming privacy concerns in consumers' use of health information technologies: A justice framework," *J. Bus. Res.*, vol. 141, pp. 782–793, 2022, doi: https://doi.org/10.1016/j.jbusres.2021.11.073.

[27] J. Ju and L. Wang, "The roles of trust and privacy calculus in citizen-centric services usage: evidence from the close contact query platform in China," *Behav. Inf. Technol.*, vol. 44, no. 3, pp. 574–595, 2025, doi: 10.1080/0144929X.2024.2330001.

[28] J. Nienstedt and M. Trenz, "From sharing to profiting: Exploring the interplay

between value creation and strategic appropriation in data ecosystems," *Electron. Mark.*, vol. 35, no. 1, p. 91, 2025, doi: 10.1007/s12525-025-00823-6.

[29] K. Shao, M. Elahi Shirvan, and A. Alamer, "How Accurate Is Your Correlation? Different Methods Derive Different Results and Different Interpretations," *Front. Psychol.*, vol. 13, p. 901412, 2022, doi: 10.3389/fpsyg.2022.901412.

[30] G. Eysenbach, "Improving the Quality of Web Surveys: The Checklist for Reporting Results of Internet E-Surveys (CHERRIES)," *J Med Internet Res*, vol. 6, no. 3, p. e34, 2004, doi: 10.2196/jmir.6.3.e34.

[31] S. Samuel and D. Mietchen, "Computational reproducibility of Jupyter notebooks from biomedical publications," *Gigascience*, vol. 13, Jan. 2024, doi: 10.1093/gigascience/giad113.

[32] N. Silaparasetty, *Machine Learning Concepts with Python and the Jupyter Notebook Environment*, 1st ed. Apress Berkeley, CA, 2020. doi: https://doi.org/10.1007/978-1-4842-5967-2.

[33] T. Kluyver, B. Ragan-kelley, and F. Pérez, "Jupyter Notebooks - a publishing for mat for reproducible computational workflows," *IOS Press / Sage Publ.*, pp. 87–90, 2016, doi: 10.3233/978-1-61499-649-1-87.

[34] F. Binsar, M. Bayu, I. Abbas, A. Budiman, and Abidah, "Analysis of Digital Content of Indonesian Society in the Public Service Sector," *Lect. Notes Networks Syst.*, vol. 1180 LNNS, pp. 87–97, 2025, doi: 10.1007/978-981-97-9324-2_8.

[35] X. Liu and L. Jiang, "How do digital platform capabilities affect service innovation in service manufacturing firms? The role of knowledge creation and environmental uncertainty.," *PLoS One*, vol. 20, no. 9, p. e0333382, 2025, doi: 10.1371/journal.pone.0333382.

[36] Y. Jia, L. Cui, J. Su, L. Wu, S. Akter, and A. Kumar, "Digital servitization in digital enterprise: Leveraging digital platform capabilities to unlock data value," *Int. J. Prod. Econ.*, vol. 278, p. 109434, 2024, doi: https://doi.org/10.1016/j.ijpe.2024.109434.

[37] H. H. Fischer, S. L. Moore, T. L. Johnson, R. M. Everhart, H. Batal, and A. J. Davidson, "Appointment reminders by text message in a safety net health care system: a pragmatic investigation," *eGEMs Gener. Evid. Methods to Improv. patient outcomes*, vol. 5, no. 1, pp. 1–8, 2017.

[38] Trevor Deley and Elizabeth Dubois, "Assessing Trust Versus Reliance for Technology Platforms by Systematic Literature Review," *Soc. Media + Soc.*, vol. 6, no. 2, p. 2056305120913883, Apr. 2020, doi: 10.1177/2056305120913883.

[39] L. Zhang, H. O. Zaki, S. Hashim, and N. A. Omar, "The role of personalization and emotional attachment on privacy calculus: an empirical study of intelligent voice assistant," *Asia Pacific J. Mark. Logist.*, vol. 37, no. 11, pp. 3113–3129, Mar. 2025, doi: 10.1108/APJML-10-2024-1578.

[40] S. Kovács and Á. Majoros-Benák, "AI-powered personalization in e-commerce: A multi-method study of consumer evaluations and campaign engagement,"

Comput. Hum. Behav. Reports, vol. 24, p. 101323, 2026, doi: https://doi.org/10.1016/j.chbr.2026.101323.

[41] N. Yildirim and B. Gündüzyeli, “The Personalization–Privacy Paradox in AI-Driven Programmatic Advertising: Implications for Digital Marketing Sustainability,” 2026. doi: 10.3390/jtaer21060179.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Additionalfile1Questionnaire.pdf