INTERNATIONAL JOURNAL OF PHARMACEUTICAL SCIENCES
[ISSN: 0975-4725; CODEN(USA): IJPS00]
Journal Homepage: https://www.ijpsjournal.com

OPEN ACCESS

Review Article

Consumer Trust vs Data Privacy in E-Pharmacies: A Systematic Review of Trade-offs in Digital Healthcare Platforms

Manoj Chendke[1], Rutuja Hivarkar[2], B. Lakshmi*

Department of Pharmaceutical Management- National Institute of Pharmaceutical Education and Research, Hyderabad

ARTICLE INFO

Published: 11 Jun. 2026

Keywords:
E-Pharmacy; Consumer Trust; Data Privacy; Privacy Paradox; Perceived Risk; Privacy Calculus; Digital Healthcare Platforms; Cybersecurity.

DOI:
10.5281/zenodo.20646392

ABSTRACT

The past few years have seen a rapid growth in online pharmacy platforms, driven by the growing digital infrastructure, the demand among the users of convenience and an increased acceptance of remote healthcare services. Although these advances have opened up a lot of value to consumers, they have also bred an impending apprehension of data security and platform reliability that directly influence whether or not individuals want to use such services. In this paper, the conflict between trust and data privacy is explored within the framework of e-pharmacy, using a systematic review of the scholarly literature on the subject over the past 20 years. This review was conducted through a search of peer-reviewed journals and conference proceedings which are indexed in Scopus, Web of Science and Google scholar with the search spanning 2003 to 2023. The analysis is especially keen on some of their mediating constructs which include perceived risk, perceived usefulness, transparency and privacy calculus framework where each of them influences how users balance the costs and benefits of using digital pharmacy services. One of the most common findings in the reviewed studies is what scholars have denoted as the privacy paradox; a behavioural paradox where consumers, despite their apparent worry about the possibility of how their personal data may be used, nonetheless utilise the e-pharmacy platforms because the perceived convenience and economic benefits of their actions supersede their concerns. Trust is a mediating variable that arises in this dynamic and modulates the relationship between the perceptions of risk and the actual usage decisions. The conclusion of this paper is that the e-pharmacy platforms that want to establish a long-term relationship with its users need to invest strategically in transparency systems, effective cybersecurity frameworks, and active privacy disclosure. These investments are not just compliance measures but strategic needs to realize sustainable growth in a progressively privacy-aware healthcare setting

***Corresponding Author:** B. Lakshmi
Address: *Department of Pharmaceutical Management- National Institute of Pharmaceutical Education and Research, Hyderabad*
Email : lakshmi.niperhyd@gov.in

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

INTRODUCTION

The combination of digital technology and healthcare has resulted in a new type of consumer service: the online pharmacy. These types of platforms enable people to buy medications, post their prescriptions, and receive health-related advice without stepping a foot inside a brick-and-mortar store. E-pharmacy adoption has been driven by high levels of smartphone ownership and rural internet penetration and a post-pandemic need to avoid physical interaction in markets such as India, where Tata 1mg and PharmEasy have already established a strong presence. [1],[2],[3].

But no one wants to adopt something because of convenience. Healthcare is a field where stakes are exceptionally high, the wrong product quality, the wrong dosage, or the mismanaged personal information may directly affect the health and safety of a person. This fact causes trust to be a far more different and more significant variable in e-commerce healthcare settings compared to, e.g., clothing or electronics stores. [4][5]. In cases where consumers are unable to touch and feel products or to check credentials in person, they need to depend on institutional cues platform reputation, certification badges, customer reviews to tune up their trust. [6].

To make matters worse, the type of data that e-pharmacies regularly gather is also a difficult aspect. Combination of prescription records, medical history, demographic identification and payment credentials makes a sensitive profile which would not likely be shared by the majority of consumers. The perceived risk of data misuse, be it through data breach, third-party data-sharing, or commercial exploitation of health records, has been long-documented to serve as an important barrier to both first and repeat use of the platform. [7]. It is not a matter of whether or not the consumers put their trust in e-pharmacies, but how they manage the conflict between the desirability of the advantages such resources can bring and the concern over the cost in terms of privacy vulnerability.

The current literature has examined trust and privacy issues in the e-commerce environment separately, yet few have been conducted to understand their interaction with each other in the digital pharmacy service context. This gap is filled through the findings in this paper, which has been compiled by two decades of empirical and theoretical studies, which seek to trace the mechanisms under which, perceived risk, transparency, security, and privacy calculus, as a collective, influence consumer trust and adoption behaviour in the e-pharmacy field.

3. Literature Review

3.1 The Nature of Consumer Trust in Online Pharmacy Platforms

Conceptual Grounding

***Corresponding Author:** B. Lakshmi
Address: *Department of Pharmaceutical Management- National Institute of Pharmaceutical Education and Research, Hyderabad*
Email : lakshmi.niperhyd@gov.in
Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Fundamentally, confidence in an e-pharmacy implies that a user is willing to rely on the assurances of the system that medications will be legitimate, deliveries will be precise, and that personal information will be managed in a responsible manner. [8]. Such a willingness does not come on a silver platter; it is achieved through experience of good interactions and it is strengthened by the plausible institutional cues. Without physical signals to the pharmacist face, the dispensing counter, the official branding of a brick-and-mortar store digital platforms will be forced to better convey reliability. [9].

Why Trust Matters Disproportionately in Healthcare

Trust influences behavior in all business spheres, but it is especially strong in healthcare. Distrusted users of an e-pharmacy will not disclose their prescriptions, will not want to finalize their purchase and will abandon the platform at the first indication that they are having a bad experience. On the other hand, high levels of trust are an incentive to share information with the user that they may not have shared otherwise, which strengthens the bond between customer and platform in the long run. The perceived trustworthiness of many e-pharmacy services is in effect virtually a requirement to the willingness to provide sensitive health data. [9].

Factors That Shape Trust Formation

The trust to digital pharmacy services has been most effectively discussed as a multidimensional construct that is influenced by a variety of discrete categories of antecedents. The reputation of the platform and brand heritage are also significant: the first trust is further extended to platforms that are related to known pharmaceutical companies or platforms which have recognisable third-party certification. Operational reliability is important as well as consistent, on-time delivery and responsive customer service add up over time to create an overall perception that the platform can be relied on. Lastly, social validation systems like confirmed customer reviews, overall satisfaction ratings, and visible communities of users decrease uncertainty that surrounds deals with new services, pushing reluctant users to participate. [10][11].

3.2 Data Privacy Concerns in the Digital Healthcare Context

Categories of Sensitive Information

E-pharmacies are placed in a rather vulnerable location in the data economy. In contrast to a typical retail site that can be aware of the address of a customer and their buying history, an e-pharmacy can store prescription information, signs of chronic conditions, medical history, and financial information at the same time. Such a stockpile of sensitive data increases the perceived stakes of any incident involving data significantly. [12].

Principal Risk Pathways

There are three types of data-related risk that are present throughout the literature. First, unauthorised intrusions caused by insufficient system defences by security breaches are the most direct threat, and can

reveal high volumes of health and financial information simultaneously. Second, commercial misuse can be described as the practice of using personal health data to conduct targeted advertising or analytics on behalf of a third party without meaningful user consent. Third, cloudy data-sharing models, where the information of the users is sent to the related organizations or government without explicit revelation, undermine the trust of the users even without an evident breach. [7]. A combination of these risk pathways makes data privacy a more pertinent issue in healthcare e-commerce than in the majority of other online retail industries. [13].

3.3 Theoretical Frameworks

Technology Acceptance Model and Its Extensions

Technology Acceptance Model Technology acceptance model is an approach suggested by Davis in 1989 which assumes that the adoption of technological system by users is basically defined by the two perceptual variables namely perceptions of usefulness (the extent to which the system is believed to increase performance) and perceptions of ease of use (the extent to which the system is believed to be effortless to use). [14]. The latter aspect is especially relevant in e-pharmacy studies where the consumer is attracted to the platform that proves to be time-efficient, less expensive, and more convenient in terms of access to medicines. Further development of the initial TAM framework, most notably the Unified Theory of Acceptance and Use of Technology, adds to the model by incorporating the social influence and enabling conditions as another determinant, which provides the framework with a wider explanatory potential in the context of studies on healthcare adoption.

Privacy Calculus

The decision to share personal information is viewed as a calculus of rational weighing of benefits and risks expected as a result of sharing personal information, as described by the theory of privacy calculus. [20]. In the case of e-pharmacies, this framework would include the economic rationality of privacy paradox: a user who appreciates the price discount, home delivery, and time savings provided by an e-pharmacy can rationally decide that the privacy risks are a price worth paying. There is a mediating role of trust in this calculation and it determines the weighting of risks and benefits in relation to each other.

Trust-Risk Framework

The trust-risk model is an inverted relationship with high risk perceptions undermining trust and the effective use of risk-mitigation strategies reinstating or strengthening trust. [15]. This model is particularly relevant to e-pharmacies since perceived risk and potential trust gains co-exist at the same time: consumers might be both concerned about data exposure and highly regard the platform, which poses a dynamic tension, which platform design and communication will have to carefully navigate.

3.4 Mediating Constructs

Perceived Risk

Perceived risk is a subjective measurement of the risk that a consumer thinks of when using a service [16]. In e-pharmacy context, this includes the paranoia of fake products, monetary fraud and mismanagement of medical records. Users will be unwilling to take risks, reduce the personal information they share, and find alternative channels even less convenient ones when they perceive the risk to be high.

Perceived Usefulness

Perceived usefulness indicates the intensity of a user to think that the platform will actually make a difference in his or her life by making it more convenient, cheaper, or quicker to access medications. [14]. Studies have continually demonstrated that perceived usefulness can counteract the trust reducing impact of privacy concerns especially when the utility payoffs are concrete and near term. An e-pharmacy consumer who spares a lot of money and time placing an order is more likely to accept moderate degrees of uncertainty regarding data processing, empirically. [17].

Transparency

Transparency refers to the degree to which a platform is very clear and easily explained in terms of their policies, price formation, data habits, and the source of their products. [18]. When the users are aware of what an e-pharmacy does with their data and why, their ambiguity will decrease, and their confidence in the intentions of the platform will increase. On the other hand, ambiguous or legalistic privacy policies, hidden data-sharing provisions and price obfuscation are indicative of institutional unreliability.

Security

Security means technical equipment encryption procedures, multi-factor authentication, safe payment gateways, and frequent system audits that websites use to safeguard user information against external assaults. [10]. Notably, security is not only about stopping any breaches but its visible application also serves as a sign of trust, to remind the users that their data is being taken seriously, even before anything bad happens.

Privacy Concern and Privacy Calculus

Privacy concern entails the subjective uneasy feeling of the user regarding the way his or her personal data would be gathered, stored, and even shared [19]. It serves as a cognitive antecedent which influences perceived risk appraisal and the decisions of information disclosure. The active evaluative process where users compare these concerns with the advantages of engagement is privacy calculus, in contrast [20]. This is mediated by trust: when one trusts a platform more, they interpret ambiguous signals more generously and are more ready to share information even though they still have some concerns.

4. Research Objectives

Primary Objective

The overall purpose of this study is to determine whether users of e-pharmacy maintain their use of the platform despite the fear of data privacy due to the utilitarian

value of convenience, savings, and accessibility that these services offer.

Secondary Objectives

1. To establish how consumer trust and willingness to embrace e-pharmacy services are influenced by the perceived usefulness.
2. To assess the role of security infrastructure and transparency measures in achieving user trust on online pharmacy sites.
3. To investigate the effect of perceived risk and privacy concern on consumer trust in e-pharmacies
4. To investigate the empirical association between privacy concern and the risk perception among users of e-pharmacies.
5. To determine the impact of the privacy calculus which is, the weighing of benefits and risks on the strength of privacy concerns of the users.
6. To quantify the effect of consumer trust on probability of adopting and maintaining e-pharmacy.
7. To test the direct impact of perceived usefulness and perceived risk on adoption by the users regardless of trust.
8. To record behavioral data on the privacy paradox by looking at the presence of concern about data privacy and continued use of the platform in the presence of benefits.

5. Hypotheses Development

This research study is based on a conceptual framework where a group of independent constructs that is seen to be useful, secure, transparent, perceived risk, and privacy concern simultaneously determine consumer trust that in turn affects consumer adoption intention. There were ten formal hypotheses that were formulated to operationalize the relational structure suggested by this framework.

5.1 Trust as the Central Outcome

Sites that seem to be useful do not need to be promoted as such, platforms that work are trusted in part because being functional is a signal that they are reliable. When a service provides what it claims to offer quicker access to medicine, cost advantages, real-time tracking users redefine their conviction of the competence and desires of the platform. This connection between trust formation and utility perception has always been documented in previous studies in digital services.

H1: The perceived usefulness has a strong positive impact on consumer trust in e-pharmacy platforms.

The encryption of security measures, authenticated logins, and secure payment processing are tangible proofs that a platform is serious about the data protection of users. They help minimize uncertainty regarding institutional purpose and minimize the psychological barriers to initial and subsequent use.

H2: Security adoption has a high positive impact on consumer confidence in e-pharmacy settings.

Easy, transparent communication regarding prices, policies and data-handling practices reduces the informational asymmetry between platform and user. The users will be in a better position to make certain and stable judgments of the platform when they are aware of the rules of engagement.

H3: Organisational communication transparency has a strong and positive impact on consumer trust on e-pharmacies.

5.2 Trust-Suppressing Factors

Perceived risk is a balancing force to trust: the higher the user believes they may be harmed by using a platform, the less likely they are to trust it. Each of these risks leads to this loss of confidence: financial, product-related, and privacy-specific.

H4: Consumer trust towards e-pharmacy platforms is negatively impacted by perceived risk to a strong degree.

The fear of data abuse on the part of the user creates a continuing background fear that disrupts the trust in the goodwill of the platform, even in a case where there is no particular incident of abuse.

H5: Privacy issue affects and has a negative impact on consumer trust of e-pharmacies.

5.3 Privacy, Risk, and Their Interrelationship

When users have concern about what might be done with their data, then they give higher likelihood estimates to the scenarios of harm or exploitation. Privacy concern may thus be perceived as a mental antecedent that increases the perceptions of risk.

H6: There is a positive and significant correlation between privacy concern and perceived risk in the e-pharmacy environment.

The trade-off calculation inherent in privacy calculus theory of the balance between expected benefits and expected risks influences the extent to which a user is concerned prior to making a decision to disclose personal information.

H7: Privacy calculus is a major determinant of the level of privacy concern as reported by e-pharmacy users.

5.4 From Trust to Adoption

The more users are convinced about a platform, the higher the chances of them fulfilling a transaction, returning to make other purchases and referring their colleagues to the service. Trust therefore acts as a gateway construct linking pre-engagement perceptions to actual adoption behaviour.

H8: Consumer trust has a significant positive effect on adoption intention among e-pharmacy users.

5.5 Direct Paths to Adoption

Beyond its effect on trust, perceived risk also discourages adoption directly, as users who anticipate harmful outcomes may opt not to

engage regardless of how much they trust the platform's intentions.

H9: Perceived risk directly and negatively impacts adoption intention in e-pharmacy settings.

Equally, high perceived usefulness can drive adoption independently of trust, particularly among pragmatic users for whom the utility gains are sufficiently compelling.

H10: Perceived usefulness directly and positively influences adoption intention among e-pharmacy users.

6. Research Methodology

6.1 Research Design

This study employed a quantitative-descriptive design, chosen for its capacity to measure relationships across multiple constructs simultaneously and to yield generalisable insights across a defined user population. The design was structured around two interrelated objectives: first, to model the causal pathways linking perceived benefits and risks to trust and adoption; and second, to document the presence or absence of the privacy paradox the condition in which privacy concern and continued platform use coexist within the sample.

6.2 Instrument Design and Data Collection

A questionnaire was created in a structured form with references to the literature on the topic of technology adoption and the information privacy which has been proven to be validated before. The tool addressed the following constructs: Perceived Usefulness, Security, Transparency, Perceived Risk, Privacy Concern, Privacy Calculus, Trust, and Adoption Intention. Each of the items was then measured in a five-point Likert response format, with responses being “Strongly Disagree”, “Strongly Agree”, to enable the clearer shades of user perception and to be cognitively manageable to the respondents.

6.3 Sampling

Data was collected among 200 respondents who confirmed they have used at least one Indian e-pharmacy site before, namely, Tata 1mg, PharmEasy, or Netmeds. Convenience sampling was chosen because of the necessity of having participants who have a relevant experience using the platform. Although this method restricts the ability to statistically generalise the results to the general population, it is necessary to make sure that responses are based on actual direct interaction with the services being tested.

6.4 Variable Classification

Independent Variables: Perceived Usefulness, Security, Transparency, Perceived Risk, Privacy Concern

Mediating Variable: Trust

Dependent Variable: Adoption Intention

Additional Variable: Privacy Calculus (used in correlation analysis only)

6.5 Analytical Techniques

All the data were analysed and processed in SPSS. There were four consecutive methods

of analysis. Firstly, the internal consistency of each measurement scale was tested through Cronbach Alpha reliability analysis to make sure that multiple items constructs were unified. Second, Pearson correlation analysis was used to test the strength and direction of the bivariate relationships, most specifically between the privacy concern and perceived risk, and between privacy calculus and privacy concern. Third, multiple linear regression has been used to develop two predictive models in which trust is the outcome variable and one in which adoption intention is the outcome variable to enable simultaneous estimation of the independent contribution of each of the predictors. Fourth, Chi-square tests cross tabulated were performed to test whether privacy concern was significantly related to the decision to use the services especially in the context of discounts, thus offering a behavioural test of the privacy paradox.

6.6 Decision Criteria for Hypothesis Testing

All hypotheses were tested at a traditional significance level of alpha = 0.05. The p-values less than this were accepted and the p-values equal or greater were rejected. The same two-tailed test was used in all inferential tests.

6.7 Integration of Analytical Approaches

The regression and Chi-square approach were a calculated choice: regression estimates the magnitude and the direction of causal effects, and Chi-square tests show whether the attitudinal variables such as the privacy concern do indeed lead to various behavioural patterns. These methods combined provide a more comprehensive view of the relationship between perceived benefits, privacy anxiety, and user decision-making as compared to either approach could have provided alone.

7. Data Analysis

7.1 Internal Consistency Assessment (Cronbach's Alpha)

Cronbach's Alpha was calculated on each construct to ensure that the questionnaire scales were measuring their constructs of interest with a certain level of consistency. The result of this statistic is in the range of 0 to 1, and the higher it is the more inter-item coherence. The common interpretive conventions that will be used in this study are as follows

Values at or above 0.90 indicate excellent internal consistency

- Values between 0.80 and 0.89 indicate good consistency
- Values between 0.70 and 0.79 indicate acceptable consistency
- Values below 0.70 are considered questionable

Table 1 below presents the reliability outcomes for each construct.

Table 1: Reliability Analysis Results

Construct	No. of Items	Cronbach's Alpha

Perceived Usefulness	3	0.82
Security	2	0.78
Transparency	2	0.72
Perceived Risk	3	0.75
Privacy Concern	2	0.80
Trust	3	0.88
Adoption Intention	2	0.90

All the seven constructs passed the acceptable reliability cut off of 0.70. The two most central constructs in the model Trust (α = 0.88) and Adoption Intention (α = 0.90) had good to excellent reliability, which confirms that these measures underpinning the model are reliable and consistent. Good internal coherence was also exhibited by Perceived Usefulness (α = 0.82) and Privacy Concern (α = 0.80). Security, Perceived Risk, and Transparency all met the acceptable standard with alpha values of 0.78, 0.75, and 0.72 respectively. These findings ensure suitability of measurement tools to be used in the regression and correlation analysis later.

7.2 Bivariate Correlation Analysis

Pearson correlation coefficients were calculated to describe bivariate relationships among privacy concern, perceived risk and privacy calculus. The correlation coefficient (r) lies between -1.00 to +1.00 whereby the values nearer to the ends show stronger relationships and those nearer to zero show weak or no linear relationship. Relations with p-values less than 0.05 were considered significant.

Table 2 presents the correlation matrix.

Table 2: Pearson Correlation Results

Variables	Privacy Concern	Perceived Risk	Privacy Calculus
Privacy Concern	1	0.52**	0.48**
Perceived Risk	0.52**	1	—
Privacy Calculus	0.48**	—	1

Note: ** denotes significance at $p < 0.05$

The relationship between privacy concern and perceived risk (r = 0.52) was statistically significant and within moderate range implying that users who are more concerned about data privacy are also more likely to give high probability to negative consequences when utilizing e-pharmacy services. This result is in line with the theoretical prediction of H6. Also, the correlation between privacy calculus and

privacy concern (r = 0.48) was also moderate and significant, meaning that the active consideration of benefits and risks contributes to the overall amount of anxiety that users have toward privacy as predicted by H7.

7.3 Regression Analysis Model 1: Determinants of Trust

In the first regression model, the cumulative impacts of five independent variables on consumer trust were studied. The relative magnitudes of the contributions of each predictor were compared using standardised beta coefficients (β) and statistical significance at the 0.05 level was determined using p-values.

Table 3 displays the regression coefficients for Model 1.

Table 3: Regression Results Determinants of Trust

Variable	Beta (β)	Sig. (p-value)
Perceived Usefulness	0.42	0.000
Security	0.30	0.001
Transparency	0.18	0.020
Perceived Risk	-0.25	0.005
Privacy Concern	-0.10	0.080

Perceived Usefulness was the most powerful positive predictor of trust ($\beta = 0.42$, $p < 0.001$). This observation indicates that in case customers think an e-pharmacy has an impactful role in improving their ability to access medicines and buy products easily, they will be significantly more inclined to trust a platform. The second most important positive predictor was security ($\beta = 0.30$, $p < 0.01$), which confirms the existence of visible and functional data protection controls as assuring users that transparent security policies, authentication schemes, and payment gateways are important factors. Although its effect was smaller ($\beta = 0.18$, $p < 0.05$), transparency was, however, statistically significant, which suggests that even the small incremental improvements in the way the platforms report on their business can increase user confidence.

As expected, Perceived Risk had a statistically significant negative impact on ($\beta = -0.25$, $p < 0.01$), which supports the main argument of the trust-risk framework. Interestingly, Privacy Concern though directionally negative ($\beta = -0.10$) was not statistically significant ($p = 0.080$), indicating that, although users might have some background apprehension about data privacy, this does not in itself have a serious enough impact on their trust to be considered significant enough to register as a regression coefficient. This can be an indication of the mediating effect of the risk perception in which the privacy concern has an indirect but not direct effect on trust.

Hypothesis outcomes for Model 1:

- H1 (Perceived Usefulness → Trust): Supported
- H2 (Security → Trust): Supported
- H3 (Transparency → Trust): Supported
- H4 (Perceived Risk → Trust): Supported
- H5 (Privacy Concern → Trust): Partially Supported directionally consistent but not statistically significant

7.4 Regression Analysis Model 2: Determinants of Adoption Intention

The second regression model evaluated the direct contributions of trust, perceived usefulness and perceived risk to adoption intention.

Table 4 shows the regression coefficients for Model 2.

Table 4: Regression Results Determinants of Adoption Intention

Variable	Beta (β)	Sig. (p-value)
Trust	0.55	0.000
Perceived Usefulness	0.35	0.000
Perceived Risk	-0.20	0.010

The most significant predictor of adoption intention was trust ($\beta = 0.55$, $p < 0.001$), which highlights the core role that relational confidence plays in the translation of positive attitudes into the real platform use. When customers believe an e-pharmacy, the chances of making purchases, revisiting the site, and sharing it in their social circles increase significantly. Perceived Usefulness also had an important predictive power in this model ($\beta = 0.35$, $p < 0.001$),, which once again confirms that functional value convenience, time savings, cost efficiency is a direct cause of adoption regardless of trust. Perceived Risk showed a strong negative influence on adoption ($\beta = -0.20$, $p < 0.01$), but relatively small compared to the positive influences of trust and usefulness, meaning that risk concerns although real are overridden as long as trust and utility are high enough.

Hypothesis outcomes for Model 2:

- H8 (Trust → Adoption Intention): Supported
- H9 (Perceived Risk → Adoption Intention): Supported
- H10 (Perceived Usefulness → Adoption Intention): Supported

7.5 Chi-Square Test Privacy Concern and Usage Decisions

A Chi-square test of independence was used to establish whether the level of privacy concern (high or low) of users influenced the probability of them still using an e-pharmacy in case tangible benefits (discounts and faster delivery) were offered. The test was also significant (χ^2, $p < 0.05$), which proved privacy concern and usage decisions to be not statistically independent.

Table 5 presents the crosstab results.

Table 5: Chi-Square Crosstab Privacy Concern vs. Usage Decision

Privacy Concern Level	Definitely Use Platform	Consider Other Options
High	70%	30%
Low	80%	20%

Even among users that had high privacy concern the findings are shocking: 70% of them would certainly use the e-pharmacy again when provided with meaningful incentives. The significance of the difference in usage intent among high-concern and low-concern users was not dramatic, although statistically significant, indicating that the effect of the perception of benefits is dramatic in reducing the behavioral implications of privacy anxiety. This trend is a definite empirical confirmation of the privacy paradox, which holds that users conduct a certain sort of rational cost-benefit calculations where convenience and economic value often prevail over apprehensions about data.

8. CONCLUSION

This paper aimed to investigate the interaction of consumer trust and data privacy issues in the context of the e-pharmacy system and to clarify whether the advantages of this type of service are high enough to keep the user interested despite existing privacy fears. The results all point at the affirmative answer to the latter question: the users of e-pharmacy seem to be primarily benefit-oriented in their choices, and trust seems to be the most important tool that the specified orientation manifests itself. The regression analyses indicate that perceived usefulness and trust are by far the most influential factors in the adoption intention whereas perceived risk though a significant deterrent has a relatively weak effect. The result that privacy concern has no significant predictive power of trust when conditioned on other variables indicates that users either decouple their privacy concerns or address them by depending on trust confirmatory cues like the reputation of the platform, security certifications, and open communication. The Chi-square analysis introduces a behavioral level to these results, showing that 70% of the users who place high levels of concern would still prefer to use the e-pharmacy platforms in case of discount and delivery deals. This tendency of worrying about privacy whilst still using it is the typical sign of the privacy paradox and it is what the privacy calculus theory predicts: when the benefits are tangible and immediate and the risks appear abstract and remote, the calculus reliably gives an advantage to the continued use. A number of practical implications of these findings are possible. E-pharmacy operators need to focus on making trust-building investments in three main areas. To start with, they ought to make investments in open communication in plain-language privacy notices, proactive disclosures on the data-sharing arrangements, and opt-out mechanisms. Second, they need to enhance security infrastructure not just as a technical backstop but as a visual signal of trust, actively communicating on the protection measures. Third, they need to seek to

optimize perceived usefulness by enhancing the user experience, providing meaningful price benefits and decrease friction in prescription and ordering process. On their part, regulators are advised to look into the establishment of minimum disclosure and audit requirements of digital pharmacy platforms, so that the structural conditions of consumer trust are not also left solely to play out in the market. The current study could be advanced fruitfully with future research exploring longitudinal variations in trust and privacy concern in more platform interactions, disaggregating results by demographic cohort like older adults or first-time users of digital health, and comparing privacy paradox dynamics in various national regulatory frameworks.

REFERENCES

1. A. Kumar, A. Adlakaha, K. Mukherjee, The effect of perceived security and grievance redressal on continuance intention to use M-wallets in a developing country, International Journal of Bank Marketing 36 (2018) 1170–1189. https://doi.org/10.1108/IJBM-04-2017-0077.
2. M. Srivastava, M. Raina, Consumers' usage and adoption of e-pharmacy in India, Int. J. Pharm. Healthc. Mark. 15 (2021) 235–250. https://doi.org/10.1108/IJPHM-01-2020-0006.
3. Healthcare System in India, Healthcare India - IBEF, (n.d.). https://www.ibef.org/industry/healthcare-india (accessed April 9, 2026).
4. D. Gefen, E. Karahanna, D.W. Straub, Trust and tam in online shopping: AN integrated model, MIS Q. 27 (2003) 51–90. https://doi.org/10.2307/30036519.
5. J. Mou, D.H. Shin, J. Cohen, Understanding trust and perceived usefulness in the consumer acceptance of an e-service: a longitudinal investigation, Behaviour and Information Technology 36 (2017) 125–139. https://doi.org/10.1080/0144929X.2016.1203024.
6. M.S. Featherman, P.A. Pavlou, Predicting e-services adoption: a perceived risk facets perspective, Int. J. Hum. Comput. Stud. 59 (2003) 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3.
7. G. Bansal, F.M. Zahedi, D. Gefen, The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online, Decis. Support Syst. 49 (2010) 138–150. https://doi.org/10.1016/J.DSS.2010.01.010.
8. D. Gefen, E. Karahanna, D.W. Straub, Trust and tam in online shopping: AN integrated model, MIS Q. 27 (2003) 51–90. https://doi.org/10.2307/30036519.
9. A. Beldad, M. De Jong, M. Steehouder, How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust, Comput. Human Behav. 26 (2010) 857–869. https://doi.org/10.1016/J.CHB.2010.03.013.
10. D.J. Kim, D.L. Ferrin, H.R. Rao, A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents, Decis. Support Syst. 44 (2008) 544–564. https://doi.org/10.1016/J.DSS.2007.07.001.
11. A.A. Alalwan, Y.K. Dwivedi, N.P. Rana, Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust, Int. J. Inf. Manage. 37 (2017) 99–110.

https://doi.org/10.1016/J.IJINFOMGT.2017.01.002.

12. G. Bansal, F.M. Zahedi, D. Gefen, The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online, Decis. Support Syst. 49 (2010) 138–150. https://doi.org/10.1016/J.DSS.2010.01.010.
13. T. Zhou, Understanding mobile internet continuance usage from the perspectives of UTAUT and flow, Information Development 27 (2011) 207–218. https://doi.org/10.1177/0266666911414596;JOURNAL:JOURNAL:IDVA.
14. F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Q. 13 (1989) 319–339. https://doi.org/10.2307/249008.
15. M.S. Featherman, P.A. Pavlou, Predicting e-services adoption: a perceived risk facets perspective, Int. J. Hum. Comput. Stud. 59 (2003) 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3.
16. P.A. Pavlou, Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, International Journal of Electronic Commerce 7 (2003) 101–134. https://doi.org/10.1080/10864415.2003.11044275.
17. V. Venkatesh, M.G. Morris, G.B. Davis, F.D. Davis, User acceptance of information technology: Toward a unified view, MIS Q. 27 (2003) 425–478. https://doi.org/10.2307/30036540.
18. A.K. Schnackenberg, E.C. Tomlinson, Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships, J. Manage. 42 (2016) 1784–1810. https://doi.org/10.1177/0149206314525202;PAGE:STRING:ARTICLE/CHAPTER.
19. H. Jeff Smith, T. Dinev, H. Xu, Information privacy research: An interdisciplinary review, MIS Q. 35 (2011) 989–1015. https://doi.org/10.2307/41409970.
20. An Extended Privacy Calculus Model for E-Commerce Transactions on JSTOR, (n.d.). https://www.jstor.org/stable/23015781 (accessed April 9, 2026).

HOW TO CITE: Manoj Chendke, Rutuja Hivarkar, B. Lakshmi*, Consumer Trust vs Data Privacy in E-Pharmacies: A Systematic Review of Trade-offs in Digital Healthcare Platforms, Int. J. of Pharm. Sci., 2026, Vol 4, Issue 6, 3030-3044. https://doi.org/10.5281/zenodo.20646392