JOURNAL OF BIOCHEMISTRY PHARMACOLOGY AND PUBLIC HEALTH

Volume: 4 Issue: 4

October-December, 2026

ISSN-2958-762X



JOURNAL OF BIOCHEMISTRY PHARMACOLOGY AND PUBLIC HEALTH
Volume: 4, Issue: 4, 2026

DOI: https://doi.org/10.64907/xkmf.v4.i4.jbpph.1

Research Article

KMF Publishers
www.kmf-publishers.com/jbpph/

OPEN ACCESS

Health Data Privacy Concerns and Conditional Willingness to Use AI Healthcare in Bangladesh

Ikhtiar Uddin Tamim[1*]; Jarin Tasnia Risha[1]; Md Al Roman[1]; Kazi Abdul Mannan[2]

[1]Department of Law; [2]Department of Business Administration
Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh

ABSTRACT

Concern about the use of health data need not imply unwillingness to engage with artificial intelligence (AI) in healthcare. This cross-sectional study examined whether concern about unauthorised data use coexisted with stated willingness under transparent data protection, and distinguished both from the importance respondents assigned to privacy in their trust judgements. The analysis used 385 adult responses to a common questionnaire on AI, health law and patient rights in Bangladesh. Five privacy items were analysed separately because they ask about different judgements. We estimated joint endorsement, compared endorsements within respondents and used exploratory adjusted regression to examine two conditional responses. Concern was endorsed by 229 respondents (59.5%); greater willingness under transparent protection was endorsed by 304 (79.0%). Both were endorsed by 182 respondents (47.3% of the sample). The willingness statement exceeded the concern statement by 19.5 percentage points (paired 95% CI 13.2 to 25.7; Holm-adjusted $p < 0.001$). Privacy protection was judged relevant to trust by 321 respondents (83.4%). None of the four focal regression coefficients met the multiplicity-adjusted threshold. The findings show that privacy concern and openness under specified conditions are compatible within the same respondents. They do not establish that making safeguards transparent increases uptake or that privacy concern predicts trust in a specific provider. The governance implication is to make protections verifiable and to evaluate concern, conditional willingness and institution-specific trust separately.

CONTACT Ikhtiar Uddin Tamim, Email: ikhtiartamim@gmail.com

ARTICLE HISTORY

Received 20 September 2026
Revised 25 October 2026
Accepted 28 October 2026
Published 30 October 2026

KEYWORDS

health data; privacy concern; conditional willingness; trust salience; artificial intelligence; Bangladesh.

Copyright: © 2026 by the authors. Licensee KMF Publishers (www.kmf-publishers.com). This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Healthcare organisations use information to make decisions, coordinate care and monitor outcomes. AI can change how that information is processed by introducing new software, additional recipients and new purposes. An application may use records to help prioritise a case, analyse an image or suggest a diagnostic possibility. Its technical performance is one consideration in deciding whether to use it. Another is whether patients can understand what information the application receives, why it receives it and who can access the resulting records. Clinical benefit and confidence in data handling can therefore diverge even when patients are asked about a single service.[1]

Health information also creates risks that can outlast the decision for which it was collected. A record created for an encounter may be stored by a hospital, transmitted to another service or accessed by a supplier under a support arrangement. A model improvement project may introduce an additional purpose. Even when each actor sees only part of the workflow, the patient experiences the service as a whole. An assurance that data are secure may leave important questions unanswered: whether a use is authorised, whether it is necessary, how long records are kept and how a disputed use can be reviewed. Security helps enforce boundaries, while privacy also concerns how those boundaries are set.

Research on privacy and acceptance often begins from the expectation that people concerned about misuse will be less willing to disclose information or use a service. That proposition can be plausible for a specified decision, but a survey can ask a different question: would a person be more willing if a protection were transparent? A person may express concern precisely because the protection matters to the decision. Conditional willingness captures openness under a stated condition without revealing a baseline willingness, an actual choice or a change caused by a specific safeguard. Conflating these measures can turn reasonable concern into an apparent obstacle to adoption and can make a favourable response to a hypothetical condition look like confidence in a real system.[2]

Likewise, judging that privacy protection strongly affects trust does not show how much a respondent trusts a provider. It signals that privacy enters the respondent's judgement. Two people can both endorse its importance while having opposite views of the same hospital. That distinction matters for an empirical design because an association with a trust-salience item cannot be interpreted as an association with institutional trust. The original instrument includes these questions in one block; the present article preserves their substantive differences.

Bangladesh's Digital Health Strategy 2023-2027 and the national FHIR implementation guide place the exchange and use of health information within a developing digital infrastructure. Standard formats can make information easier to transfer and interpret. They do not independently establish permission for a transfer, certify a supplier or determine which records a particular user may access. The governance issue is how organisations make the intended boundaries of

[1] World Health Organization, Ethics and Governance of Artificial Intelligence for Health (WHO 2021); Baptiste Vasey and others, ‘Reporting Guideline for the Early-Stage Clinical Evaluation of Decision Support Systems Driven by Artificial Intelligence: DECIDE-AI’ (2022) 28 Nature Medicine 924.

[2] Tamara Dinev and Paul Hart, ‘An Extended Privacy Calculus Model for E-Commerce Transactions’ (2006) 17 Information Systems Research 61; Mary J Culnan and Pamela K Armstrong, ‘Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation’ (1999) 10 Organization Science 104.

exchange visible to people whose information moves through the system.[3]

The Personal Data Protection Act 2026 includes health-related information within sensitive personal data and defines health data broadly. This provides a legal context for distinguishing data about a person's condition from other personal information collected while delivering care. The legal classification is separate from whether a respondent considers a particular use appropriate. A questionnaire about preferences cannot verify compliance, and the existence of a statutory category does not demonstrate that people know what it covers or can exercise relevant rights.[4]

This study asks three questions. How frequently do respondents endorse concern about unauthorised health-data use, strong protection, information about relevant uses, conditional willingness and privacy's importance to trust? How often do concern and conditional willingness occur together, and how do the item endorsements compare within respondents? Finally, how do concern and the two protection expectations covary with conditional willingness and trust salience after adjustment for recorded background differences?

The answers support a narrower contribution than a causal model of institutional assurance. The central evidence is the joint distribution: it identifies individuals who report concern and conditional openness together. The adjusted analysis then asks whether variation in the original ratings tracks either of the two conditional responses. It is possible for a combination to be common without showing a strong statistical relationship; two high marginal endorsements may overlap substantially even when the variables are only weakly related. Reporting both types of evidence keeps that distinction visible.

The data come from a common Group 12 questionnaire. Other titles use the same records to address diagnostic acceptance and medical-error accountability. This study instead focuses on what respondents say about health-data use, safeguards and conditional willingness. Its contribution is distinct in question and analysis, while the shared data source means the papers are not independent samples.

2. Literature Review and Theoretical Foundation

The framework combines privacy calculus, procedural assurance and appropriate reliance. Each addresses a different part of a decision about health AI. Privacy calculus directs attention to what people expect to gain or risk. Procedural assurance concerns what institutions do to make their commitments credible. Appropriate reliance asks whether confidence is directed towards the right actor and matched to available evidence. The questionnaire addresses parts of these ideas, and the analysis distinguishes those parts from concepts it cannot measure.

[3] Directorate General of Health Services, Digital Health Strategy 2023–2027 of Bangladesh <https://dghs.gov.bd/pages/static-pages/6922dfd6933eb65569e243cd> accessed 3 November 2026; Directorate General of Health Services, Bangladesh Core FHIR Implementation Guide (version 0.5.0) <https://fhir.dghs.gov.bd/core/> accessed 3 November 2026.

[4] Personal Data Protection Act 2026 (Bangladesh), Act No 63 of 2026, ss 1(3), 2(21)(f) and 2(22).

2.1 Health data protection as a condition of service use

Health AI may operate on identifiable records, pseudonymised extracts or other data, depending on the service and its design. A model used in one clinical decision may receive information different from the information used to develop or maintain it. A patient who agrees to a clinical procedure may have a different view about using related records to train a model for future customers. A useful distinction is therefore between the immediate clinical purpose and other proposed processing. Organisations should be able to identify which purposes are necessary for care, which are optional and which actors carry responsibility for each. The distinction is especially important when an AI function is embedded in a general digital service and is not apparent to the person receiving care.[5]

Technical protection and transparency serve different roles. Access controls can limit who reads a record; clear information can explain why the access exists and what a person can do if it is disputed. One is not evidence of the other. A plain-language notice can describe practices that are poorly implemented, while well-designed controls may be invisible to patients. Treating HPT2 and HPT3 as separate descriptive items makes this distinction observable. Their average in the secondary analysis is a deliberately simple summary of endorsement of protection expectations, not a measure of a provider's demonstrated performance.

2.2 Privacy calculus and procedural fairness

Dinev and Hart model decisions to disclose in electronic commerce as depending on considerations that include perceived risk and trust. The relevance to health AI is that concern can persist when a person sees value in a service and considers the conditions under which it is offered. The clinical context also limits the analogy. A shopper may be able to leave a website easily; a person seeking urgent care may have no comparable alternative. Even when several providers are available, practical costs can reduce freedom to choose. A response expressing greater willingness under transparent protections should therefore not be read as consent to exchange a right for a benefit. It indicates that the stated condition matters to the respondent's hypothetical choice.[6]

Culnan and Armstrong connect procedural fairness with impersonal trust. Their account directs attention to the procedures by which information is handled rather than relying solely on personal familiarity with the actor. In a health service, assurance could arise from procedures such as an accessible account of how data are used, clear responsibilities for each recipient and an effective channel for questioning a use. The evidence needed to establish this kind of assurance would include what the institution does, what the person knows and whether the procedure can be used. The present questionnaire asks whether some of these protections should exist. It does not present procedures for respondents to evaluate or measure whether they believe a real provider applies them.[7]

[5] WHO, Ethics and Governance (n 1); World Health Organization, Regulatory Considerations on Artificial Intelligence for Health (WHO 2023).
[6] Dinev and Hart (n 2).
[7] Culnan and Armstrong (n 2).

Privacy concern is also broader than fear of unauthorised access. Measurement research distinguishes dimensions such as collection, awareness and control. A respondent may regard the collection itself as excessive even if all subsequent access is authorised. Another may welcome collection for care but object to transfer for a different purpose. HPT1 captures an important concern about unauthorised use, but does not map these judgements or measure the subjective probability of a breach. The study's empirical statements are accordingly limited to the recorded concern.[8]

2.3 Appropriate reliance and the target of trust

Trust has a target and a context. Confidence in the competence of a diagnostic system does not necessarily imply confidence in the hospital's information governance, and confidence in a hospital does not imply confidence in every supplier it employs. Trust in automation research emphasises matching reliance to the system's capacities and the circumstances of use. Research on trust measurement similarly distinguishes beliefs about a trustee from intentions to depend on it. These distinctions help explain why HPT4 and HPT5 should remain separate. HPT4 identifies greater willingness under a stated condition. HPT5 records whether respondents consider privacy protection consequential to trust. Neither identifies a trustee, rates its actual performance or establishes behaviour.[9]

The point is not to maximise reported trust at all costs. A person may appropriately withhold reliance until a provider identifies the uses of a record, or may choose to rely on a system for one task while retaining reservations about a different use. Technical and organisational evaluation are needed to establish whether such reliance is warranted. A survey can inform how safeguards should be communicated and evaluated, but cannot substitute for evidence about how a provider acts.[10]

2.4 Accountability and the ability to question data use

An accountability perspective asks who must provide an explanation and who can review it. In a data flow involving a hospital and an external service, the patient may not know whether a disputed use originated with the clinical team, the hospital's procurement arrangement or a vendor process. A visible route for questions helps identify the responsible actor. For the route to be credible, whoever handles the request must be able to reconstruct the use, consult appropriate records and respond within their authority. The presence of a privacy notice may support this process, but it does not establish that the route can obtain answers.[11]

This matters when translating privacy protection into public confidence. A promise can be assessed only to the extent that a person understands its scope and can identify what would happen if it were breached. The survey's conditional language makes transparency salient, but does not specify whether transparency refers to a notice, an independent audit or the ability to inspect a record. This ambiguity is analytically important. Different respondents can agree with the same statement while expecting quite different institutional practices. A future design can manipulate or describe those practices separately rather than using a broad assurance statement as an intervention.

[8] Naresh K Malhotra, Sung S Kim and James Agarwal, ‘Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model’ (2004) 15 Information Systems Research 336.

[9] John D Lee and Katrina A See, ‘Trust in Automation: Designing for Appropriate Reliance’ (2004) 46 Human Factors 50; D Harrison McKnight, Vivek Choudhury and Charles Kacmar, ‘Developing and Validating Trust Measures for e-Commerce: An Integrative Typology’ (2002) 13 Information Systems Research 334.

[10] WHO, Ethics and Governance (n 1); Karim Lekadir and others, ‘FUTURE-AI: International Consensus Guideline for Trustworthy and Deployable Artificial Intelligence in Healthcare’ (2025) 388 BMJ e081554.

[11] Mark Bovens, ‘Analysing and Assessing Accountability: A Conceptual Framework’ (2007) 13 European Law Journal 447.

2.5 Conceptual framework and expectations

Figure 1 describes the analytical framework. Privacy concern is a judgement about unauthorised use. Protection and information expectations describe what respondents think institutions should provide. Conditional willingness and trust salience are separate response measures. The arrows represent exploratory statistical associations. Paired comparisons examine the items' endorsements within respondents and do not impose a temporal sequence.

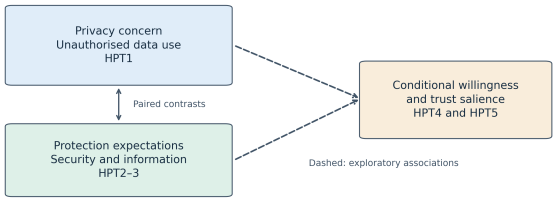

Figure 1. Analytical framework for privacy concern and conditional responses

There are competing expectations. Concern could coincide with lower willingness because individuals see health data use as risky even when protections are described. It could also coincide with higher conditional willingness if respondents perceive safeguards as addressing a concern. A weak association is possible if the conditional wording gives concerned and unconcerned respondents different reasons to agree. The study therefore examines the joint distribution before interpreting regression.

Protection expectations may be positively associated with conditional willingness because a person who values transparency may respond favourably when it is made explicit. They may also be associated with trust salience because respondents attach importance to privacy when judging providers. Such associations could reflect common wording or an underlying tendency to endorse protective policies. They cannot establish a causal role for actual safeguards. No confirmatory latent model, mediation or moderation is specified after observing this already collected dataset.

3. Methodology

The analysis applies the supplied questionnaire to a set of questions that can be answered by its observed items. It describes both the empirical procedures and the limits of the source documentation. The reporting follows the logic of cross-sectional observational reporting by specifying denominators, adjustment choices and the interpretation of uncertainty.[12]

3.1 Design and sample

The Group 12 workbook contains a Data sheet, a codebook and a README linking the questionnaire to three research titles. The unit of analysis is an individual response. The study uses a cross-sectional adult questionnaire concerning AI, health law and patient rights; it does not link responses to health records, use logs or named healthcare providers. The workbook contains 385 records, all included in the analyses. Each record has affirmative responses for consent, adult eligibility and general AI awareness. These eligibility fields do not verify previous use of AI healthcare.

The source documents do not establish an invitation denominator, sampling frame, exact dates, verified distribution mode or study-specific pilot procedures. A response rate, population weight or probability-sample margin of error is therefore unavailable. We report the achieved analytical sample and its composition. There is no retrospective power or finite-population calculation used to certify representativeness.

[12] Erik von Elm and others, 'The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) Statement: Guidelines for Reporting Observational Studies' (2007) 4 PLOS Medicine e296.

3.2 Screening and scope

We checked the uniqueness of the record sequence, the consent and eligibility fields, blanks in the analysed variables and the permitted ranges of the agreement ratings. The 20 agreement fields contained values from 1 to 5, and there were no duplicate response and profile patterns after excluding the sequence and contextual-text fields. “None” is a valid response to the AI tool item. No deletion was based on agreement patterns. The authors identified the synthetic descriptors for the sequence and contextual fields as metadata labelling errors and confirmed the numerical responses as empirical. Contextual text was excluded from the analysis and is neither quoted nor used to establish sample characteristics.

3.3 Measurement

Table 1 distinguishes item content from analytical role. HPT1 measures agreement with concern about unauthorised use. HPT2 and HPT3 respectively concern strong protection and clear information about data use. Their equal-weight mean is the expectations summary used in regression. HPT4 and HPT5 are analysed separately as conditional willingness and trust salience. Neither enters the explanatory summary, so a positive result cannot arise from including an outcome item in its own predictor.

Table 1. Analytical roles of privacy and adjustment items

Role	Code	Interpretation
Concern	HPT1	Concern about unauthorised use
Protection expectation	HPT2	Normative support for strong privacy and security
Information expectation	HPT3	Normative support for information about data use
Conditional willingness	HPT4	Greater stated willingness if protection is transparent
Trust salience	HPT5	Reported importance of privacy protection for trust
Adjustment	AIL1-3 and profile	Observed AI orientation, status, location and training

The expectation mean averages HPT2 and HPT3 only. Neither outcome enters the predictors.

Appendix A reproduces the wording and response anchors. No item is reverse-coded: concern is retained as concern, not interpreted as negative trust. The HPT block's coefficient alpha and rank correlations are reported descriptively to assess whether pooling would obscure heterogeneous item content. Alpha is not a test of dimensionality and does not establish a formative measurement model. The expectation mean is an observed summary, while all substantive comparisons retain the component statements. The study makes no claim of validated multi-item measures of privacy concern or trust.[13]

[13] Klaas Sijtsma, ‘On the Use, the Misuse, and the Very Limited Usefulness of Cronbach’s Alpha’ (2009) 74 Psychometrika 107.

3.4 Joint endorsement and within-person comparisons

Agreement or strong agreement defines endorsement. Counts for all five categories are reported, so readers can see how many responses lie on either side of the reporting threshold. Wilson intervals accompany the marginal proportions. A cross-tabulation compares HPT1 and HPT4 to identify co-endorsement. Non-endorsement includes neutrality and is not interpreted as opposition. Counts and percentages use the same 385 respondents.[14]

Four paired contrasts compare endorsement of each HPT2-5 statement with HPT1. The difference equals the number endorsing only the comparator minus the number endorsing only concern, divided by the sample size. Exact McNemar tests condition on discordant pairs. Pointwise 95% intervals come from 10,000 percentile bootstrap resamples of whole respondents using seed 20261103. The four test probabilities form one Holm family. These contrasts describe differences between statements with different objects; they are not rankings of interchangeable indicators of one attitude.[15]

3.5 Exploratory associations

Two adjusted linear models use the original 1-5 ratings for HPT4 and HPT5. Each includes HPT1, the mean of HPT2-3, the mean of AIL1-3 and categorical indicators for current status, location and training. AIL1-3 describe recognition of plausible inaccuracy, reported verification and recognition of bias. Their average is a background orientation summary rather than tested literacy. Status, location and training describe profile differences and are not treated as a sufficient confounder set for causal inference. HC3 standard errors address heteroskedasticity under the working model. The four focal coefficients across both outcomes form a single Holm family. Intervals are pointwise.[16]

Two sensitivity models focus on willingness. Logistic regression models endorsement of HPT4 with robust sandwich intervals, retaining the same predictors. The linear specification is also repeated among respondents classified as law students; the constant status category contributes no contrasts in this subset. Each sensitivity model uses a two-coefficient Holm family. Differences in precision or significance across the subset and full sample are not tests of heterogeneity. The binary model changes the estimand by collapsing strong agreement and agreement.[17]

[14] Edwin B Wilson, ‘Probable Inference, the Law of Succession, and Statistical Inference’ (1927) 22 Journal of the American Statistical Association 209.

[15] Quinn McNemar, ‘Note on the Sampling Error of the Difference between Correlated Proportions or Percentages’ (1947) 12 Psychometrika 153; Bradley Efron and Robert J Tibshirani, An Introduction to the Bootstrap (Chapman & Hall 1993); Sture Holm, ‘A Simple Sequentially Rejective Multiple Test Procedure’ (1979) 6 Scandinavian Journal of Statistics 65.

[16] Halbert White, ‘A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity’ (1980) 48 Econometrica 817; Holm (n 15).

[17] David W Hosmer Jr, Stanley Lemeshow and Rodney X Sturdivant, Applied Logistic Regression (3rd edn, John Wiley & Sons 2013); Ronald L Wasserstein and Nicole A Lazar, ‘The ASA Statement on p-Values: Context, Process, and Purpose’ (2016) 70 American Statistician 129.

3.6 Ethics and data protection

The analysed records concern questionnaire responses, not patient files or clinical interventions. Every analysed record carries affirmative consent and adult eligibility. The analysis retains only information needed for the quantitative questions, does not use free text and reports findings in aggregate. No study-specific formal approval or exemption was documented in the available materials. The use of consent indicators and limited reporting describes safeguards for this analysis and does not imply that a formal review took place.

4. Results

The results first describe the sample and item distributions. The joint analysis then identifies respondents who endorse both concern and conditional willingness. Finally, the regression results show whether differences in the original ratings track differences in conditional responses after adjustment. Each primary analysis uses the same 385 records.

4.1 Respondents

Table 2 presents the profile fields most relevant to interpretation. The largest age group was 21-23 (150, 39.0%); 248 respondents (64.4%) were aged 21-26. The status field recorded 118 law students, 52 law graduates and 61 advocates or legal professionals. The remaining 154 were described as other relevant respondents. Dhaka accounted for 147 records, and district towns for 104. In total, 216 respondents reported no formal AI training, while 122 reported a short orientation and 47 a course or certified training.

Table 2. Sample profile

Characteristic	Category	n (%)
Age	21-23	150 (39.0%)
Age	24-26	98 (25.5%)
Age	18-20	60 (15.6%)
Age	31+	41 (10.6%)
Age	27-30	36 (9.4%)
Status	Other relevant respondent	154 (40.0%)
Status	Law student	118 (30.6%)
Status	Advocate or legal professional	61 (15.8%)
Status	Law graduate	52 (13.5%)
Location	Dhaka	147 (38.2%)
Location	District town	104 (27.0%)
Location	Other city corporation	71 (18.4%)
Location	Upazila-rural area	52 (13.5%)
Location	Other	11 (2.9%)
AI training	No	216 (56.1%)
AI training	Yes, short orientation	122 (31.7%)
AI training	Yes, course or certified training	47 (12.2%)

Denominator = 385 for all percentages.

The profile gives useful context without identifying the sample as patients. Sixty per cent were classified in the three law-related status groups. The residual category does not identify occupation or prior healthcare use. General AI awareness was universal by eligibility, but awareness of a general-purpose tool is not evidence that a respondent has used an AI-enabled health service. The findings should therefore be read as responses to questionnaire statements in this mixed adult sample.

4.2 Responses to the privacy statements

Table 3 shows that 229 respondents (59.5%) endorsed concern about unauthorised use. Another 138 chose neutrality, and 18 selected one of the two disagreement categories. Strong protection was endorsed by 313 respondents (81.3%), while clear information about data use was endorsed by 250 (64.9%). These items differ in both wording and observed distribution. In particular, 127 respondents strongly agreed with protection and 57 strongly agreed with information.

Table 3. Distributions of health privacy and conditional response ratings

Item	1	2	3	4	5	Agree n (%)	95% CI (%)
HPT1	1	17	138	168	61	229 (59.5%)	54.5 to 64.3
HPT2	0	7	65	186	127	313 (81.3%)	77.1 to 84.9
HPT3	1	22	112	193	57	250 (64.9%)	60.0 to 69.5
HPT4	0	6	75	174	130	304 (79.0%)	74.6 to 82.7
HPT5	0	4	60	165	156	321 (83.4%)	79.3 to 86.8

Agree combines 4 and 5. Intervals are Wilson intervals.

Greater willingness under transparent protection was endorsed by 304 respondents (79.0%), including 130 in the highest category. Privacy protection's importance to trust was endorsed by 321 (83.4%), including 156 who strongly agreed. Four respondents disagreed with the trust-salience statement and none strongly disagreed. A ceiling tendency in such an item limits its ability to differentiate respondents who all consider privacy important for different reasons.

The coefficient alpha across HPT1-5 was 0.238. The largest pairwise Spearman correlation was 0.125 between HPT2 and HPT3. The rank correlation between concern and conditional willingness was –0.011; between concern and trust salience it was 0.016. These are descriptive statistics, not evidence of a validated factor structure. The weak relationships are consistent with treating the statements separately for interpretation.

4.3 Co-endorsement of concern and conditional willingness

Table 4 shows that 182 respondents endorsed both concern and conditional willingness, equivalent to 47.3% of all respondents. Among the 229 who endorsed concern, 182 (79.5%) also endorsed conditional willingness. Among the 156 who did not endorse concern, 122 (78.2%) endorsed conditional willingness. The similarity of these conditional percentages is compatible with substantial overlap and little marginal discrimination by concern.

Table 4. Joint endorsement of concern and conditional willingness

Concern about unauthorised use	Willingness not endorsed	Willingness endorsed	Total
Not endorsed	34 (8.8%)	122 (31.7%)	156 (40.5%)
Endorsed	47 (12.2%)	182 (47.3%)	229 (59.5%)
Total	81 (21.0%)	304 (79.0%)	385 (100.0%)

Cell percentages use the full sample. Non-endorsement includes neutral responses.

Forty-seven respondents endorsed concern without endorsing conditional willingness, while 122 endorsed conditional willingness without endorsing concern. Thirty-four endorsed neither. These patterns show that concern and conditional openness coexist, but the coexistence itself is not evidence that concerned respondents are especially likely to become willing. The high proportion endorsing conditional willingness in both concern groups is central to interpreting the overlap.

4.4 Paired endorsement contrasts

Table 5 compares each statement with concern about unauthorised use. Protection exceeded concern by 21.8 percentage points. This difference came from 131 respondents who endorsed protection without endorsing concern and 47 who did the reverse. The information statement exceeded concern by 5.5 points, with a pointwise interval from −1.3 to 12.2 points and an adjusted p value of 0.133.

Table 5. Paired contrasts with concern about unauthorised use

Contrast	Other only	Concern only	Gap (pp)	95% CI (pp)	Holm p
HPT2 – HPT1	131	47	21.8	15.3 to 28.1	<0.001
HPT3 – HPT1	99	78	5.5	-1.3 to 12.2	0.133
HPT4 – HPT1	122	47	19.5	13.2 to 25.7	<0.001
HPT5 – HPT1	130	38	23.9	17.7 to 30.1	<0.001

Exact McNemar tests. Pointwise percentile intervals use 10,000 respondent resamples.

The willingness statement exceeded concern by 19.5 points (95% CI 13.2 to 25.7), based on 122 versus 47 discordant responses. Trust salience exceeded concern by 23.9 points (95% CI 17.7 to 30.1), based on 130 versus 38 discordant responses. Protection, willingness and trust salience all retained adjusted p values below 0.001. These comparisons identify the relative breadth of endorsement for the statements as written. They do not establish that participants value one specific protection more than another in a clinical choice.

4.5 Adjusted associations and sensitivity

Table 6 reports the estimates for concern and protection expectations. For conditional willingness, the adjusted concern coefficient was −0.014 (95% CI −0.104 to 0.076). For trust salience it was 0.009 (95% CI −0.085 to 0.102). Both are near zero on the 1-5 scale under the fitted models. The expectation summary had an adjusted willingness coefficient of 0.162 (95% CI 0.018 to 0.305); its Holm-adjusted p value was 0.111. The pointwise interval and adjusted p value address different error rates. The expectation coefficient for trust salience was 0.090 (95% CI −0.053 to 0.233; Holm-adjusted p = 0.649).

Table 6. Adjusted associations with conditional willingness and trust salience

Model (n)	Term	Estimate	95% CI	Holm p	R^2
Willingness rating (385)	Concern	-0.014	-0.104 to 0.076	1.000	0.092
Willingness rating (385)	Expectations	0.162	0.018 to 0.305	0.111	0.092
Trust salience rating (385)	Concern	0.009	-0.085 to 0.102	1.000	0.027
Trust salience rating (385)	Expectations	0.090	-0.053 to 0.233	0.649	0.027
Willingness endorsement (385)	Concern	1.085	0.796 to 1.479	0.605	0.086
Willingness endorsement (385)	Expectations	1.381	0.838 to 2.278	0.411	0.086
Law students willingness (118)	Concern	0.095	-0.071 to 0.261	0.521	0.156
Law students willingness (118)	Expectations	0.127	-0.202 to 0.456	0.521	0.156

Linear rows report unstandardised coefficients, HC3 intervals and ordinary R^2. Binary willingness rows report odds ratios, sandwich intervals and McFadden pseudo-R^2. Holm families: four main coefficients together, two coefficients separately for each sensitivity

model.

The full models explained 9.2% of the observed variance in willingness and 2.7% in trust salience. These values describe fit in the analysed data, not prediction for new respondents. No focal term met the Holm-adjusted 0.05 threshold. In the willingness endorsement model the concern odds ratio was 1.085 (95% CI 0.796 to 1.479), and the expectations odds ratio was 1.381 (95% CI 0.838 to 2.278). Among law students, the linear coefficients were 0.095 for concern and 0.127 for expectations, with intervals spanning zero. The sensitivity analyses do not supply independent confirmation of an association, and the estimates do not establish equivalence. The more direct evidence concerns the overlap and item-level contrasts.

5. Discussion

The central finding is that concern about unauthorised use and openness under transparent protection commonly occur together. Nearly half of the sample endorsed both statements. This is useful evidence against classifying concerned respondents as uniformly unwilling to engage with AI-enabled healthcare. It does not establish that transparency changes willingness. The conditional wording was presented to everyone, and no respondent faced a randomly assigned alternative or reported an observed change in behaviour.

5.1 Coexistence and the privacy calculus

Privacy calculus provides one way to understand the joint responses. A person can recognise a risk and still consider a service worthwhile when appropriate protections are in place. The survey's conditional item leaves the benefits, costs and decision setting unspecified, so it cannot estimate a calculus or show how people trade privacy against clinical value. Coexistence is a narrower observation. It matters because an instrument that forces concern and acceptance onto opposite ends of one scale would fail to represent the 182 respondents who endorsed both.[18]

The similar conditional willingness percentages in the two concern groups make the distinction especially clear. About four fifths of each group said they would be more willing if protections were transparent. Thus the overlap does not show that concerned respondents react more favourably to transparency than others. Nor does it reveal the willingness of either group under current practice. A respondent could move from unwilling to somewhat willing without choosing the service. Another could already be willing and still report that clearer protections would strengthen that position. Measuring willingness with and without a specified safeguard in a controlled design would distinguish these interpretations.

The survey also does not show a behavioural privacy paradox. It records two self-reported judgements at one time, and the judgements are compatible. Calling the responses inconsistent would imply a contradiction that is not present in the item wording. In a healthcare setting, recognising concern as compatible with engagement can help providers take questions seriously rather than dismissing them as resistance. Whether a response changes after an explanation, however, is an empirical question

[18] Dinev and Hart (n 2); Malhotra, Kim and Agarwal (n 8).

for a different design.

5.2 Strong protection and clear information

A broad commitment to strong privacy and security received considerably more endorsement than concern about unauthorised use. The clear-information item had a smaller gap from concern and did not retain adjusted evidence of a difference. These observations suggest that an endorsement rate for a general protective principle cannot substitute for evidence about a particular information practice. The items vary in abstraction and wording, and respondents were not asked to rank them or trade one for another. A survey should therefore avoid translating these percentages into a spending priority.

A procedural fairness perspective nevertheless gives the contrast practical meaning. Protection can include controls that patients never observe. Information can help them understand which protections apply and when those protections may be questioned. Giving information without establishing enforceable practice can create unwarranted confidence, while effective controls that are never explained may leave people unable to make an informed judgement. Research on procedural fairness suggests why both visible procedures and their implementation deserve attention. The observed responses identify candidate elements for testing, not evidence that a specific notice is credible.[19]

The information statement may also evoke different expectations depending on prior experience. Someone familiar with digital systems may imagine a detailed account of recipients and purposes. Another may simply want to know whether any external company receives their record. The questionnaire does not distinguish these interpretations. Testing comprehension in realistic care scenarios would help determine whether respondents can find and use the information they say should be provided.

5.3 Trust salience and exploratory models

The strongest endorsement was for the proposition that privacy protection strongly affects trust. This result shows that respondents consider privacy relevant when judging healthcare AI. It does not estimate the level of trust, confidence in a particular provider or the degree of warranted reliance. Trust measurement research distinguishes beliefs about a trustee from willingness to depend on it; automation research further distinguishes reliance that matches the system's capacities from indiscriminate reliance. A survey of trust in health AI should identify who or what is trusted and for which activity.[20]

The adjusted models yielded little evidence of a stable association of concern with either conditional response. An expectations coefficient for willingness was positive in the main linear model, but the pointwise interval excluding zero did not correspond to significance after adjustment across the four focal coefficients. The binary and student analyses did not sharpen that result. These estimates should not be taken as proof that concern and protection expectations are irrelevant. Single-item measures, a narrow response range and mixed respondent backgrounds may limit what the models can detect. Common protective wording may also account for part of the positive expectations coefficient.

The low coefficient alpha and weak correlations are consistent with the distinction between content domains. They do not identify the reason

[19] Culnan and Armstrong (n 2); WHO, Regulatory Considerations (n 5).
[20] Lee and See (n 9); McKnight, Choudhury and Kacmar (n 9).

for the observed pattern. It could reflect truly distinct judgements, differences in how items are read or both. This is why the descriptive contrasts take priority over interpreting a small set of regression coefficients as a causal model. The data support a substantive argument about how to report these questions and a methodological argument for improving how they are measured.

5.4 Implications for interpreting the Bangladesh context

Bangladesh's digital health strategy and interoperability work provide a context in which health data can move across organisational boundaries. These developments make the difference between technical exchange and authorised exchange salient. A standard can help systems interpret a field consistently; it does not resolve whether a recipient should access it for a particular purpose. The survey's broad support for protection makes it reasonable to include governance information when evaluating those services. It does not indicate that respondents understand the underlying standard or that providers implement its protections uniformly.[21]

The Personal Data Protection Act 2026 gives health-related data a specific statutory classification. Section 1(3) distinguishes provisions deemed effective from sections 23 and 31-35, which are subject to later commencement by notification under the provision. The analysis does not treat the Act as evidence that all procedures are currently available or that a particular clinical system meets statutory requirements. An operational assessment would need the relevant provisions and any implementing instruments, together with evidence about actual data use. The article uses the legislation to identify the legal relevance of the subject, while the survey describes what this sample endorsed.[22]

6. Theoretical and Practical Implications

The findings support evaluating privacy governance and conditional responses at different levels. The first concerns what protection a service can substantiate. The second concerns how users interpret and respond to that protection. Improving the second without examining the first can raise confidence without establishing that it is warranted.

6.1 Theory and measurement

A useful extension of privacy calculus research would measure separately the perceived probability of unauthorised use, the severity of the consequences, the value of the clinical service, and whether a credible alternative is available. Concern as recorded here is neither a probability estimate nor a measure of all those components. Conditional willingness is also not baseline intention. A model that includes both baseline willingness and responses to clearly specified conditions would provide a firmer test of whether assurance changes a decision.[23]

Procedural assurance can then be operationalised through beliefs about an identified provider or the availability of verifiable procedures. Trust measures should distinguish competence in delivering care from confidence in the provider's data handling. A patient could accept a clinician's judgement while remaining uncertain about retention by a vendor. Using separate measures allows that combination to be expressed. The contribution of the current findings is to show why the distinctions matter empirically, not to claim that the instrument validates a new latent theory.[24]

[21] DGHS, Digital Health Strategy (n 3); DGHS, FHIR Guide (n 3).
[22] Personal Data Protection Act 2026.
[23] Dinev and Hart (n 2); Malhotra, Kim and Agarwal (n 8).
[24] Culnan and Armstrong (n 2); McKnight, Choudhury and Kacmar (n 9); Lee and See (n 9).

6.2 Service design and oversight

A provider introducing an AI-supported service could document which health data the system needs for the immediate clinical task, where it processes them and whether any other use is proposed. Patient-facing information can answer the same questions in ordinary language and identify a contact for clarification. A notice should be tested for comprehension: can a patient identify who receives the information and whether an optional use can be declined? These questions are more concrete than asking whether the notice appears reassuring. Privacy information should also be usable by people who do not rely on a smartphone or who need assistance in another language.[25]

The institutional work behind the notice includes testing access controls, reviewing permissions when roles change and maintaining records of transfers or vendor access where appropriate. If the provider makes a claim about retention or secondary use, it needs a way to check that claim against operational practice. Procurement documents can specify the purposes for which a supplier receives data, any permitted onward processing, how retention is reviewed and which party can respond to a patient query. An accountability route should identify who can investigate when information about a use is incomplete. These are design recommendations; their suitability depends on the service and applicable requirements.[26]

6.3 Evaluation and policy

Evaluators can ask whether a person understands the stated use, can identify the responsible organisation and knows where to raise a concern. A separate outcome can record whether the person chooses the service after receiving that information. Operational evidence should examine whether documented uses match actual data flows and whether staff can investigate a disputed use. These measures would allow a provider to distinguish a clear explanation from a well-functioning safeguard. The present survey supports including those questions in an evaluation; it does not identify which notice format or intervention will work best.[27]

7. Conclusion Limitations and Future Research

Concern about unauthorised health-data use was compatible with conditional willingness in this Bangladesh questionnaire sample. Of 385 respondents, 182 endorsed both concern and greater willingness if data protections were transparent. Strong protection and the relevance of privacy to trust also attracted broad endorsement. Regression did not identify a focal association that survived multiplicity adjustment. The evidence therefore describes a common response pattern and the relative endorsement of separate statements, rather than a model in which privacy risk or assurance is shown to change trust.

The sample includes a large share of people in legal study or practice, and prior use of a clinical AI service was not verified. Recruitment dates, a sampling frame and an invitation denominator were unavailable. The results are not estimates for Bangladesh's patient population. The questionnaire does not measure actual data practices, an independent baseline for willingness or trust in an identified institution.

[25] WHO, Ethics and Governance (n 1); Bangladesh Medical and Dental Council, Telemedicine Guidelines (July 2020) section 5.8.1.
[26] Bovens (n 11); WHO, Regulatory Considerations (n 5).
[27] DGHS, FHIR Guide (n 3); Lekadir and others (n 10).

Using one concern item and heterogeneous expectation items restricts interpretation of adjusted associations. Shared response anchors may introduce common response tendencies. No longitudinal evidence establishes direction of association, and the companion Group 12 studies use the same records.

A follow-up could recruit adults with verified exposure to specific AI-enabled services and document recruitment separately for patients, clinicians and other stakeholders. Interviews could establish what people understand by transparency and unauthorised use. A vignette study could then vary the clarity of information, use of identifiable data, secondary-use options and independent oversight. It should measure trust in an identified actor, comprehension and a concrete service choice separately, and specify the comparator before analysis. Repeating these measures after a real encounter would help assess whether stated conditional openness predicts use. This programme would connect expressed preferences with the capacity of institutions to deliver protections people can understand and verify.

Declarations

Ethical approval and oversight

No study-specific formal ethics approval or exemption was documented in the available study materials. The analysis concerns a non-interventional adult questionnaire. Section 3.6 describes the recorded consent indicators, exclusion of contextual text and aggregate reporting.

Informed consent

All 385 analysed records contain affirmative consent and adult eligibility responses.

Data availability

Requests for de-identified numerical data and analysis specifications may be directed to the corresponding author. Sharing is subject to participant confidentiality and applicable institutional requirements.

Funding and competing interests

No external funding or competing interest was disclosed in the available study materials.

Author contributions

Ikhtiar Uddin Tamim led the student research, developed the research question, organised the study materials and prepared the initial manuscript. Prof. Dr Kazi Abdul Mannan supervised the study, provided conceptual and methodological guidance, contributed to the interpretation and critically revised the manuscript. Kazi Abdul Mannan is the corresponding author.

Generative AI disclosure

Generative AI assisted literature retrieval, manuscript development, language editing and preparation of analysis code. Numerical estimates were computed programmatically from the supplied workbook. The authors are responsible for verifying and approving the analysis, interpretation and reporting.

Bibliography

Bangladesh Medical and Dental Council, *Telemedicine Guidelines* (July 2020) section 5.8.1

Bovens M, ‘Analysing and Assessing Accountability: A Conceptual Framework’ (2007) 13 European Law Journal 447

Culnan MJ and Armstrong PK, ‘Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation’ (1999) 10 Organization Science 104

Dinev T and Hart P, ‘An Extended Privacy Calculus Model for E-Commerce Transactions’

(2006) 17 Information Systems Research 61

Directorate General of Health Services, *Bangladesh Core FHIR Implementation Guide* (version 0.5.0) <https://fhir.dghs.gov.bd/core/> accessed 3 November 2026

Directorate General of Health Services, *Digital Health Strategy 2023-2027 of Bangladesh* <https://dghs.gov.bd/pages/static-pages/6922dfd6933eb65569e243cd> accessed 3 November 2026

Efron B and Tibshirani RJ, *An Introduction to the Bootstrap* (Chapman & Hall 1993)

Holm S, 'A Simple Sequentially Rejective Multiple Test Procedure' (1979) 6 Scandinavian Journal of Statistics 65

Hosmer DW Jr, Lemeshow S and Sturdivant RX, *Applied Logistic Regression* (3rd edn, John Wiley & Sons 2013)

Lee JD and See KA, 'Trust in Automation: Designing for Appropriate Reliance' (2004) 46 Human Factors 50

Lekadir K and others, 'FUTURE-AI: International Consensus Guideline for Trustworthy and Deployable Artificial Intelligence in Healthcare' (2025) 388 BMJ e081554

Malhotra NK, Kim SS and Agarwal J, 'Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model' (2004) 15 Information Systems Research 336

McKnight DH, Choudhury V and Kacmar C, 'Developing and Validating Trust Measures for e-Commerce: An Integrative Typology' (2002) 13 Information Systems Research 334

McNemar Q, 'Note on the Sampling Error of the Difference between Correlated Proportions or Percentages' (1947) 12 Psychometrika 153

Sijtsma K, 'On the Use, the Misuse, and the Very Limited Usefulness of Cronbach's Alpha' (2009) 74 Psychometrika 107

Vasey B and others, 'Reporting Guideline for the Early-Stage Clinical Evaluation of Decision Support Systems Driven by Artificial Intelligence: DECIDE-AI' (2022) 28 Nature Medicine 924

von Elm E and others, 'The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) Statement: Guidelines for Reporting Observational Studies' (2007) 4 PLOS Medicine e296

Wasserstein RL and Lazar NA, 'The ASA Statement on p-Values: Context, Process, and Purpose' (2016) 70 American Statistician 129

White H, 'A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity' (1980) 48 Econometrica 817

Wilson EB, 'Probable Inference, the Law of Succession, and Statistical Inference' (1927) 22 Journal of the American Statistical Association 209

World Health Organization, *Ethics and Governance of Artificial Intelligence for Health* (WHO 2021)

World Health Organization, *Regulatory Considerations on Artificial Intelligence for Health* (WHO 2023)

Appendix A Questionnaire wording

Table A1 gives the exact wording of the focal privacy statements and the three items used to summarise general AI orientation.

Table A1. Exact wording of the analysed questionnaire statements

Code	Questionnaire statement
AIL1	I understand that generative AI can produce plausible but inaccurate information.
AIL2	I verify important AI-generated information before relying on it.
AIL3	I understand that AI outputs may reflect bias or incomplete data.
HPT1	I am concerned about unauthorized use of health data by AI systems.

Code	Questionnaire statement
HPT2	Health data used for AI should receive strong privacy and security protection.
HPT3	Patients should receive clear information about relevant uses of their health data.
HPT4	I would be more willing to use AI healthcare services if data protections were transparent.
HPT5	Privacy protection strongly affects my trust in AI-enabled healthcare.

Source: Group 12 Codebook. Response anchors run from 1 strongly disagree to 5 strongly agree.

HPT4 and HPT5 are separate outcomes. HPT2 and HPT3 contribute to the expectation mean; neither establishes that a real service provides the stated safeguard.

Table of Legislation

Personal Data Protection Act 2026 (Bangladesh), Act No 63 of 2026, ss 1(3), 2(21)(f) and 2(22)