Information Management and Business Review (ISSN 2220-3796)
Vol. 18, No. 4(S), pp. 237-250, 2026

A Privacy Trade-off Model for Older Adults' Digital Health Disclosure in Malaysia: The Moderating Role of Persuasion Functions

*Melissa Shahrom[1], Norshima Humaidi[1], Ramita Abdul Rahim[1], Farah Syazreena Azmi[1], Siti Diyana Binti Ibrahim[2]
[1]Department of Technology and Supply Chain Management Studies, Faculty of Business and Management, Universiti Teknologi MARA, Puncak Alam Campus, Malaysia
[2]Jabatan Kesihatan Negeri Selangor, Jalan Persiaran Kayangan, Wisma Sunway, Shah Alam, Malaysia
Email: *melissa@uitm.edu.my
Corresponding Author: Dr Melissa Shahrom

Abstract: This conceptual paper develops a privacy trade-off model to explain older adults' willingness to disclose personal health information through mobile health applications with electronic health record (EHR)-related functions in Malaysia. It focuses on the trade-off between perceived privacy risk and perceived benefit and on the proposed moderating role of persuasion functions. The paper integrates privacy calculus theory and cognitive dissonance theory with the manuscript's review of gerontechnology, electronic health records, trust, information sensitivity, perceived benefits and four persuasion paradigms: free choice, induced compliance, hypocrisy and effort justification. Fourteen hypotheses are organized into a conceptual framework, followed by a proposed two-phase empirical validation plan. The proposed model positions perceived privacy risk and perceived benefit as the central trade-off mechanisms underlying stated willingness to disclose, rather than observed disclosure behavior. Information sensitivity and trust are linked to privacy risk, while service availability, critical mass, compatibility and complementarity are linked to perceived benefit. The four persuasion paradigms are proposed as moderators of the perceived privacy risk and information disclosure relationships. The model brings privacy calculus and cognitive dissonance perspectives together in a gerontechnology context and applies them to older adults' personal health-information disclosure in Malaysia, connecting digital-health adoption, privacy, persuasion and inclusive digital transformation within one conceptual framework.

Keywords: *Digital healthcare; gerontechnology; electronic health records; privacy calculus; cognitive dissonance; information disclosure; older adults; MySejahtera; Malaysia*

1. Introduction and Background

Gerontechnology is an interdisciplinary field that combines gerontology and technology to address the health, cognitive, and social needs of ageing populations through user-centred design. Gerontological design seeks efficient solutions that enhance older adults' quality of life by applying gerontological insights and design research to understand their preferences and needs (Huang & Oteng, 2023). Its solutions and applications aim to support health, independence, social participation, and quality of life among older adults (Huang & Oteng, 2023; Halicka & Surel, 2021). As populations age, gerontechnology is increasingly relevant to active ageing and efforts to reduce unnecessary dependence on traditional healthcare delivery (Huang & Oteng, 2023).

The benefits of gerontechnology do not automatically translate into adoption. Older adults may also experience barriers associated with digital literacy, technology complexity, usability, and confidence when interacting with digital systems (Yan & Xing, 2025; Huang & Oteng, 2023). These barriers are particularly important in digital healthcare, where users are often asked to provide sensitive information through applications and connected health services. The value of a technically capable system therefore depends partly on whether users consider it understandable, trustworthy and safe enough to use.

Healthcare records management is one area in which digital technologies can support older adults. Electronic health records (EHRs) have increasingly replaced or supplemented paper-based records as healthcare organizations manage larger volumes of patient information (Highfill, 2019). Health information systems can improve access to clinical information, record mobility and decision-making, while well-managed digital records can support continuity and quality of care (Wang et al., 2018; Nguyen et al., 2014; Kruse & Beane, 2018). These benefits are especially relevant for older adults who may require long-term follow-up and coordination across multiple healthcare providers.

EHR use also raises concerns about privacy, security and confidentiality. Poor security practices, insufficient protection measures and vulnerable infrastructure may result in sensitive patient information being exposed and heightening concern about the consequences of data misuse (Kruse et al., 2017; Hall & McGraw, 2014). For older adults, such concerns can combine with technology anxiety, uncertainty, and a sense of vulnerability, thereby decreasing their readiness to take part in digital health services (An et al., 2025). The main issue is therefore not just whether digital health systems can provide services efficiently, but also whether the users are willing to disclose the personal information needed by those services. Additionally, it is essential to involve users in matters of privacy and security in healthcare. If healthcare professionals let users take an active role in protecting their medical records, this will help them to understand their rights and responsibilities in relation to privacy. Offering suitable tools and resources can increase confidence in digital health platforms and lessen the uncertainty about how to protect personal information (Paul et al., 2023).

The model focuses on patient-facing mobile health applications that ask older adults to enter, update or share EHR-related personal health information for their own care. It does not examine automatic sharing between healthcare providers or data collected without an active disclosure decision. Throughout the paper, willingness to disclose refers to a person's stated intention to provide information in such an application, not evidence that the information has actually been shared.

2. Literature Review and Model Development

Gerontechnology and the privacy disclosure dilemma

Older adults' disclosure decisions reflect a tension between expected benefits and perceived barriers. Users may be more willing to share health information when they trust a digital health application and expect benefits such as convenience, better access to care, or continuity of treatment. At the same time, concerns about fraud, misuse, and loss of control can discourage disclosure (An *et al.*, 2025). Therefore, a straightforward rejection of technology and digital systems can be mitigated by persuasive approaches.

Digital literacy shapes how confidently older adults interact with digital platforms. Greater familiarity can make information requests and privacy settings easier to interpret, whereas limited familiarity may increase uncertainty. Security concerns, scams and misinformation can further weaken confidence in digital platforms. Trust and perceived benefits also matter, as users are more likely to participate when they view a health information system as useful, reliable and capable of supporting healthcare outcomes (Kisekka & Giboney, 2018; Verheij et al., 2018; Nilashi et al., 2016). These factors remain important even when a system is technically sophisticated because personal health information is sensitive and its disclosure depends heavily on users' judgement.

A technically efficient health system can therefore remain underused when the disclosure process does not address users' concerns. The highly personal nature of health information means that adoption depends on more than usability or service availability. For instance, users must also decide whether the expected value of participation is sufficient to justify giving a digital platform access to information they regard as private. This tension is especially important for older adults because uncertainty about surveillance, scams, fraud or misuse may reinforce reluctance even when the healthcare purpose is understood. The disclosure decision should consequently be examined as part of technology acceptance itself rather than as a separate administrative step. This study therefore addresses two connected questions. First, what factors discourage older adults from allowing personal health information to be digitized? Second, what factors encourage disclosure despite privacy concerns? The proposed model examines the antecedents of perceived privacy risk and perceived benefit, the effects of those perceptions on willingness to disclose personal health information, and the role of persuasion functions in changing the relationship between perceived privacy risk and information disclosure. The contribution is to bring these risk–benefit judgements together with four distinct cognitive-dissonance-related conditions and to consider whether each condition changes the discouraging effect of privacy risk on disclosure willingness among older adults in Malaysia. This combines an established privacy trade-off explanation with a specific set of proposed boundary conditions in a setting where health information is particularly sensitive.

Digital health and EHR context in Malaysia

Health record management is increasingly shaped by data-driven healthcare systems, integrated care platforms and digital records. This shift increases the importance of accurate and timely information disclosure for personalized care, remote monitoring and continuity of treatment. It can also intensify concerns about privacy and the risks of digital engagement, particularly among older users (Malarvizhi *et al.*, 2024). Understanding disclosure willingness is therefore part of the broader challenge of making digital healthcare inclusive rather than merely technically available.

Malaysia has invested in health information infrastructure for several years. In 2016, the Ministry of Health introduced the Malaysian Health Data Warehouse (MyHDW), a centralized platform that consolidates data from multiple health information systems (Ministry of Health Malaysia, 2016). Digital health systems can improve access to records and support clinical decision-making, but their value depends on the quality, security and responsible use of the information they contain. These issues are particularly significant for older adults whose care may involve repeated consultations and long-term health management.

Among older adults, the advantages of integrated health information are strongly linked to continuity of care. Timely access to records is particularly valuable for repeated consultations, chronic-condition management and coordination between healthcare providers. However, the transfer of information across digital platforms can increase concerns regarding who can view, reuse, or share those records. The resulting challenge is therefore twofold: digital health infrastructure must ensure that relevant information is accessible when required while also providing users with sufficient assurance that access is both controlled and transparent. Consequently, this balance makes privacy perception a direct issue for participation in digital healthcare rather than only a technical security concern.

Malaysia's wider digital-health environment also illustrates the practical tension between access and privacy. Older adults can benefit from mobile health services, yet adoption may still be affected by limited digital literacy, privacy concerns and fear of technology misuse (Malarvizhi *et al.*, 2024). Supportive interfaces, caregiver assistance and focused digital-literacy initiatives may reduce practical barriers, but they do not remove the need for clear consent and credible privacy protection. For this reason, disclosure behavior should be examined as a social and behavioral dimension of digital-health transformation.

Privacy is especially important in gerontechnology because many applications process sensitive personal and health information. Perceived misuse can threaten users' sense of autonomy and control. The willingness of older adults to participate in digital-health services therefore depends not only on functionality but also on whether the system creates an acceptable balance between expected benefits and perceived privacy risk (Sun et al., 2024).

Attitudes towards disclosing personal health information

Attitudes towards health-information disclosure vary across individuals. Some users are comfortable sharing health details, while others may hesitate because of privacy concerns, social stigma or information sensitivity (Robinson, 2018). Health information disclosure should therefore be treated as a personal decision. At the same time, the disclosure of accurate information can reduce unnecessary repetition, improve record availability and support continuity of care. Boise *et al.* (2013) examined older adults' willingness to share health-related data and their privacy concerns after exposure to technology-based in-home monitoring. Their findings indicate that privacy concerns do not necessarily result in complete avoidance of digital health technologies. Instead, disclosure may remain acceptable when users perceive a legitimate and beneficial healthcare purpose. Hence, the policy challenge is to obtain the information needed for effective services without weakening autonomy or confidence.

The privacy trade-off perspective proposes that individuals compare perceived risks with expected benefits before disclosing personal information. In gerontechnology, older adults may be more willing to disclose when the anticipated benefits of health support, safety or connectivity are judged to outweigh privacy-related concerns. This trade-off provides the organizing logic for the proposed model.

Perceived benefits of disclosing health data

Potential benefits of health-data disclosure include more personalized healthcare, greater engagement in health management, improved access to information and a stronger sense of control over care. Digital records can also support continuity and potentially reduce avoidable costs when information is available to appropriate healthcare providers (Highfill, 2019; Kruse & Beane, 2018). The model proposes four antecedents of perceived benefit: number of services, perceived critical mass, perceived compatibility and perceived complementarity.

The number of services available through a digital health platform can influence whether users consider the platform useful. A broader set of relevant services can increase the perceived value obtained from disclosure. Accordingly, the first hypothesis is:

H1: A higher number of available services is positively associated with perceived benefit.

Perceived critical mass refers to a user's perception that technology has achieved sufficiently widespread adoption to become socially established. It captures the point at which adoption becomes self-sustaining and participation increases (Ford *et al.*, 2009; Centola *et al.*, 2018). Reaching critical mass requires technology to offer clear value, appeal to a sufficiently broad group, and remain accessible. For older adults, observing use by peers, family members or healthcare providers may reduce uncertainty and signal that a digital health platform is useful and socially supported. This reasoning leads to:

H2: Perceived critical mass is positively associated with perceived benefit.

Perceived compatibility concerns the extent to which technology fits users' needs, preferences and established ways of performing tasks. Older adults are more likely to perceive value when a digital health service aligns with their expectations and can be incorporated into existing routines (Amadea & Indrawati, 2022). Evidence from other digital-service settings offers a starting point for this proposition; its relevance to older adults' mobile health use still needs to be tested. Compatibility with users' health-information practices and quality-of-life goals may therefore strengthen their willingness to use the technology. Accordingly:

H3: Perceived compatibility is positively associated with perceived benefit.

Perceived complementarity refers to the extent to which the components of an EHR environment, such as software, data and connected services, are viewed as working together to produce better outcomes. It is particularly relevant when care involves multiple providers or systems because the usefulness of one component can depend on how well it works with others (Politi *et al.*, 2022). Hence:

H4: Perceived complementarity is positively associated with perceived benefit.

H5: Perceived benefit is positively associated with willingness to disclose personal health information.

Perceived privacy risk of disclosing health data

Health information is highly sensitive, and users may hesitate to disclose it when they are uncertain about how it will be collected, used, stored, or shared. Concerns can arise from possible misuse, unauthorized access, loss of control and doubts about confidentiality. Security and privacy challenges in EHR environments therefore have behavioral consequences in addition to technical consequences (Alanazi et al., 2015; Keshta & Odeh, 2021; Kruse et al., 2017). Information sensitivity and trust are consequently positioned as important antecedents of perceived privacy risk, while both constructs are also expected to influence disclosure willingness directly.

H6: Higher information sensitivity is positively associated with perceived privacy risk.

H7: As the sensitivity of the requested information increases, willingness to disclose personal health information decreases.

H8: Trust in the platform is negatively associated with perceived privacy risk.

H9: Trust in the platform is positively associated with willingness to disclose personal health information.

H10: Perceived privacy risk is negatively associated with willingness to disclose personal health information.

H10 is the baseline relationship: higher perceived privacy risk is expected to be associated with lower willingness to disclose. H11–H14 examine whether the strength of that negative relationship changes under four different persuasion conditions. A positive interaction in this model would mean that the negative risk–willingness slope becomes less steep; it would not mean that privacy risk has a positive direct effect on willingness.

Theoretical foundations

Privacy, security and confidentiality remain central challenges in EHR implementation (Alanazi et al., 2015; Keshta & Odeh, 2021). Privacy concerns the individual's ability to exercise control over personal information, whereas security concerns the mechanisms used to restrict unauthorized access. The transition from paper-based to electronic records has expanded the number of settings in which health information can be accessed, transmitted and combined, increasing the need for governance and technical safeguards (Rothstein, 2007; Sittig & Singh, 2010).

Privacy calculus theory explains disclosure as a decision in which individuals weigh anticipated benefits against perceived risks (Keith *et al.*, 2013). Cognitive dissonance theory provides a complementary explanation for situations in which behavior conflicts with beliefs or attitudes. A person who believes that disclosure is risky may nevertheless decide to share information to obtain a valued service, creating psychological tension that can influence subsequent attitudes or behavior (Festinger, 1957; Cooper, 2019; McGrath, 2017).

Together, the two theories support the core logic of a privacy trade-off model. Privacy calculus explains why benefits and risks are evaluated, while cognitive dissonance provides a basis for examining how conditions surrounding a disclosure decision may alter the relationship between the evaluations and behavior. The proposed persuasion functions are therefore treated as moderators rather than as substitutes for the underlying privacy risk mechanisms.

Both theories also recognize that the same disclosure situation can be interpreted differently by different individuals. The privacy-calculus evaluation depends on the perceived consequences and advantages attached to a particular request, while dissonance becomes relevant when the action taken does not sit comfortably with an existing belief or attitude. In the present context, an older adult may believe that sharing health information creates privacy risk and still decide to disclose because access to a digital-health service is considered beneficial. The resulting tension provides the conceptual basis for examining whether conditions of choice, compliance, self-consistency or invested effort alter the strength of the risk and disclosure relationships.

Table 1: Theoretical integration in the proposed model

Theory	Core decision mechanism	Model elements	Proposed explanatory role
Privacy calculus theory	Users weigh anticipated benefits against perceived privacy risks before disclosure.	Perceived benefit; perceived privacy risk; willingness to disclose	Explains why risk and benefit evaluations shape disclosure willingness.
Cognitive dissonance theory	Psychological tension can arise when disclosure behavior conflicts with beliefs or attitudes.	Free choice; induced compliance; hypocrisy; effort justification	Explains why conditions surrounding disclosure may alter the risk and disclosure relationships.

Persuasion functions

In this study, persuasion functions refer to cognitive-dissonance-related paradigms that may influence how users respond to perceived privacy risk when deciding whether to disclose their personal health information. Their relevance lies in the possibility that the same level of perceived risk may not lead to the same disclosure decision under different conditions of choice, compliance, self-consistency, or invested effort. Therefore, persuasion functions are proposed to moderate the negative association between perceived privacy risk and willingness to disclose personal health information. The proposed model focuses on the analysis of four persuasion functions which are free choice, induced compliance, hypocrisy and effort justification.

Free choice paradigm

The free choice paradigm emphasizes perceived freedom in making a decision (Brehm, 1956; Risen & Chen, 2010). It is the degree to which individuals see the decision about the disclosure of their health information as a voluntary one and thus do not experience any pressure to take any action. In a digital disclosure setting, users

should be able to determine whether to provide information, understand the consequences of the choice, and modify or withdraw consent where appropriate. When users perceive genuine choice and control, the negative effect of privacy risk on disclosure willingness may be reduced because the decision is experienced as voluntary rather than imposed. Accordingly:
H11: The free choice paradigm positively moderates the relationship between perceived privacy risk and willingness to disclose personal health information, such that the negative effect is weakened when perceived choice is high.

Induced compliance paradigm
The induced compliance paradigm examines situations in which individuals engage in behavior that is inconsistent with an existing attitude and subsequently experience pressure to restore consistency (Risen & Chen, 2010; Cancino-Montecinos et al., 2018). In other words, induced compliance is seen when individuals are encouraged to do something that conflicts with their beliefs. The degree of choice and the explanation given for a request can affect whether an initial act of disclosure leads people to reconsider their earlier reservations. In digital-health environments, these conditions require particular caution because the platform should not make users feel that disclosure is compulsory when meaningful consent is expected.

A related sequential-request strategy is the foot-in-the-door technique (Burger, 1999). It begins with a small request that is relatively easy to accept, followed by a larger related request. The logic is that initial compliance can increase the likelihood of subsequent compliance. In this model, the relevant possibility is that an earlier, freely accepted and low-pressure request may prompt a person to view a later request more favorably despite perceived privacy risk. This is a proposed change in the risk–willingness relationship, not a claim that pressure or large incentives necessarily improve disclosure. Thus:
H12: The induced compliance paradigm positively moderates the relationship between perceived privacy risk and willingness to disclose personal health information, such that the negative relationship is weaker when an earlier, low-pressure disclosure decision encourages consistency with that voluntary choice.

Hypocrisy paradigm
The hypocrisy paradigm draws attention to inconsistency between standards that individuals endorse and their previous behavior. It refers to the discrepancy between beliefs concerning privacy that individuals tend to hold, and their actual actions such as disclosure of personal health information through mobile applications. Making such inconsistency salient can motivate efforts to restore consistency (Gauld *et al.*, 2021). Applied to privacy decisions, users may compare their stated privacy concerns with their previous disclosure behavior or with the benefits they expect from a digital service. The framework therefore proposes that self-inconsistency can alter the effect of perceived privacy risk on willingness to disclose. Accordingly:
H13: The hypocrisy paradigm positively moderates the effect of perceived privacy risk on willingness to disclose personal health information, reducing the negative impact when users experience self-inconsistency.

Effort justification paradigm
Effort justification suggests that people may evaluate an outcome more positively when they have invested substantial time or effort in obtaining it (Harmon-Jones & Mills, 1999; McGrath, 2017). In a digital-health context, users who have invested effort in registration, verification or completing health-related information may place greater value on the resulting service. Where users regard that effort as worthwhile, they may become less reluctant to share information despite perceived privacy risk. The proposed effect therefore concerns a weaker negative risk–willingness relationship, rather than a positive direct effect of privacy risk. This should not be interpreted as support for burdensome registration or pressure to continue after investing effort. Hence:
H14: The effort justification paradigm positively moderates the relationship between perceived privacy risk and willingness to disclose personal health information, such that the negative relationship is weaker when users perceive their earlier effort in using the system as worthwhile.

Moderating role of persuasion functions
Older adults may experience uncertainty in digital environments because of limited familiarity, reduced confidence or concerns about vulnerability. Clear explanations of how information is collected, protected and used can reduce ambiguity and improve risk comprehension. Persuasion, however, should not be treated as a

mechanism for overcoming privacy concerns at any cost. Its role should be to support informed judgement, strengthen perceived control and make the consequences of disclosure easier to understand (Sun et al., 2026).

Perceived privacy risk generally suppresses disclosure willingness, while control and trust can support participation (Keith et al., 2013). The effect of risk may therefore vary according to how a disclosure request is framed and how much autonomy a user perceives. It may also vary when an earlier voluntary disclosure, recognition of inconsistency or worthwhile invested effort changes how a person interprets the request. These variations provide the rationale for modelling the four persuasion paradigms as moderators.

Poorly designed persuasion can have the opposite effect. Complex explanations, exaggerated assurances or coercive design can increase skepticism and reinforce risk-avoidant behavior. The proposed model therefore treats persuasion as conditional: its effect depends on the specific paradigm and on whether the design respects autonomy, transparency and user comprehension. This is particularly important for older adults because persuasive mechanisms should support rather than exploit vulnerability.

The four paradigms offer different explanations for the same proposed moderation of H10: free choice concerns control over a decision; induced compliance concerns consistency following an earlier voluntary action; hypocrisy concerns awareness of a gap between stated beliefs and previous actions; and effort justification concerns the value attached to effort already invested. Each interaction remains a hypothesis to be tested. The direction may differ in practice if users perceive pressure, manipulation, or a loss of control.

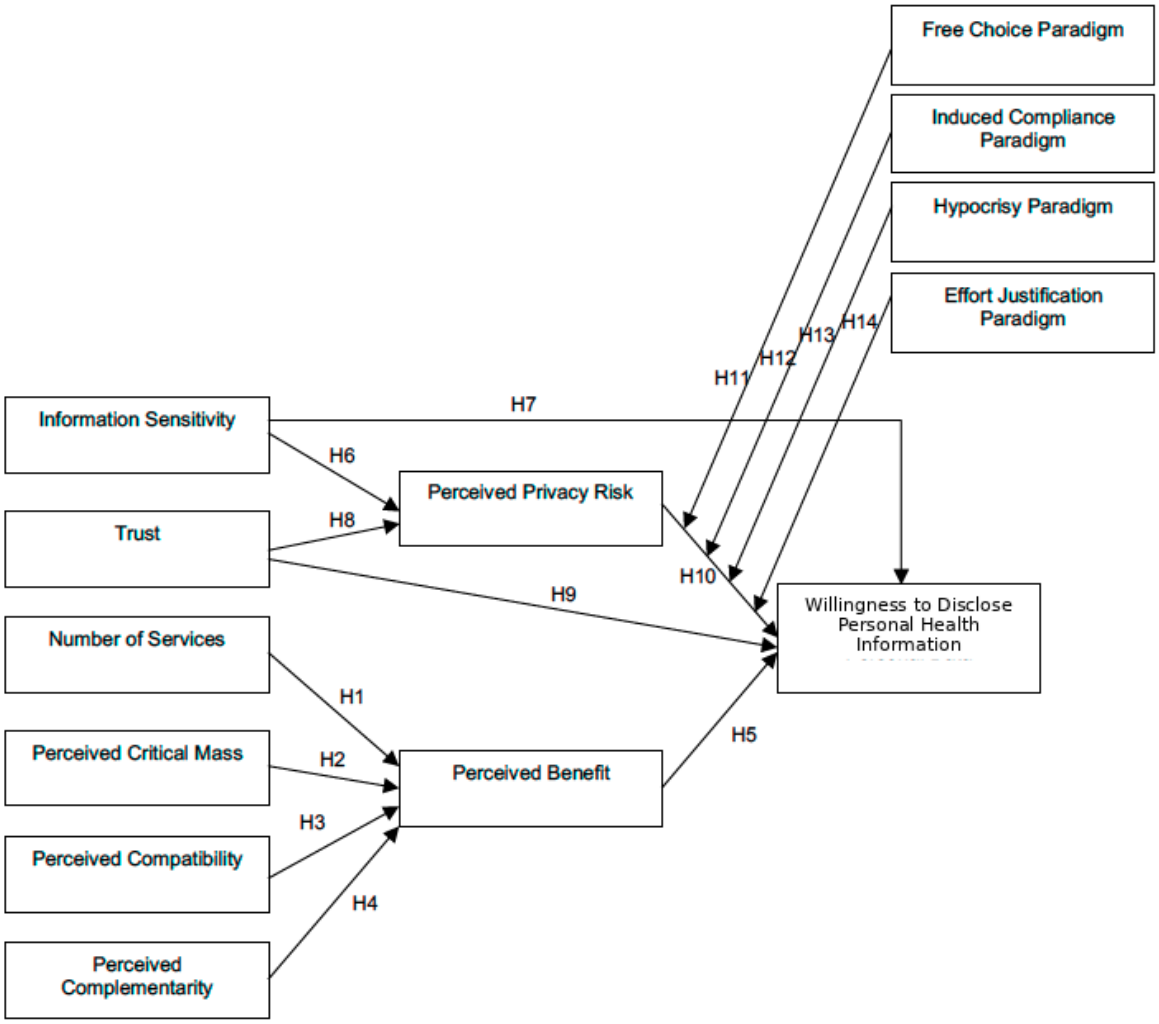
Table 2: Persuasion functions and proposed moderating relationships

Persuasion function	Condition	Moderated relationship	Proposed effect
Free choice	Perceived freedom and control in deciding whether to disclose	Privacy risk → willingness to disclose	Weakens the negative effect when perceived choice is high (H11).
Induced compliance	Earlier voluntary disclosure under a low-pressure request, followed by a desire for consistency	Privacy risk → willingness to disclose	Weakens the negative risk–willingness relationship after an earlier voluntary, low-pressure disclosure (H12).
Hypocrisy	Salient inconsistency between endorsed standards and previous behavior	Privacy risk → willingness to disclose	Reduces the negative effect when self-inconsistency is experienced (H13).
Effort justification	Effort already invested in registration, verification or providing information that is seen as worthwhile	Privacy risk → willingness to disclose	Weakens the negative risk–willingness relationship when earlier effort is seen as worthwhile (H14).

Conceptual framework

Figure 1 summarizes the proposed privacy trade-off model. Perceived privacy risk and perceived benefit form the central trade-off mechanisms. Information sensitivity and trust are linked to perceived privacy risk; number of services, perceived critical mass, perceived compatibility, and perceived complementarity are linked to perceived benefit; and trust and information sensitivity also have direct relationships with disclosure willingness. The four persuasion paradigms are positioned as moderators of the perceived privacy risk and disclosure relationships.

Figure 1: Proposed privacy trade-off model



3. Proposed Empirical Validation

Because the present article is conceptual, the empirical procedures described in this section are proposed for subsequent validation of the framework rather than reported as completed research. The proposed design has two phases. Phase 1 is intended to refine the contextual relevance of the framework and the measurement instrument, while Phase 2 is intended to test the hypothesized relationships quantitatively.

Phase 1: preliminary qualitative study

Phase 1 proposes interviews with approximately three to five key stakeholders from relevant Malaysian health and cybersecurity organizations. The purpose is to explore factors that may contribute to older adults' willingness or reluctance to disclose personal health information and to assess whether the conceptual factors identified from the literature require contextual refinement.

These stakeholder interviews are intended as a preliminary check on the wording and contextual relevance of the proposed constructs, rather than as a source of findings about older adults as a whole. Before the main survey, draft questions will also be tried with a small group of older adults through brief cognitive interviews or think-aloud checks to see whether the consent scenarios, privacy terms and response options are clear.

RQ1: What factors make older adults reluctant to disclose personal health information and allow it to be digitized?

RO1.1: To identify factors that make older adults reluctant to disclose personal health information and allow it to be digitized.

The interview data are proposed to be analyzed thematically and mapped against the literature-derived constructs. The resulting themes would be used to refine the privacy trade-off framework and support questionnaire development. Measurement items would be adapted from prior research where appropriate, with any self-developed items subjected to expert review and instrument pre-testing before the second phase. Participants in these pre-tests will be asked to explain how they understand key terms such as trust, privacy risk and voluntary disclosure. Their comments will be used to revise unclear wording and remove questions that are difficult to answer. No results from these preliminary activities are presented in this conceptual article.

Phase 2: quantitative model testing

Phase 2 proposes a survey of adults aged 60 years or older who use smartphones in selected urban and semi-urban locations in central Malaysia, including Selangor, Kuala Lumpur, Putrajaya and Cyberjaya. Purposive sampling is proposed to identify respondents who fit the study criteria and are able to engage with a specific mobile health application, which is MySejahtera.

RQ2: Which factors contribute to older adults' willingness to disclose personal health information in the context of privacy concerns?

RO2.1: To examine the proposed direct relationships among the model constructs, including factors associated with perceived privacy risk and perceived benefit and their effects on older adults' willingness to disclose personal health information through patient-facing mobile health applications.

RO2.2: To examine whether the free choice, induced compliance, hypocrisy and effort justification paradigms each moderate the relationship between perceived privacy risk and willingness to disclose personal health information.

The survey will use a clearly described voluntary EHR-related disclosure scenario, so respondents are answering about the same kind of request. Trust will be assessed through items on the perceived reliability of the application or provider, confidence in how information is handled and confidence that privacy commitments will be honored. Willingness to disclose will be measured through intention items about providing the requested information in that scenario. Previous disclosure habits will be recorded separately through self-reported frequency of digital-health information sharing, the types of information previously provided and whether respondents have declined earlier requests. These reports describe experience; they are not independently observed disclosure behavior and will not be substituted for the main outcome. Perceived privacy risk, perceived benefit and each persuasion paradigm will be measured with distinct, literature-informed multi-item scales, checked for clarity and validity before model testing.

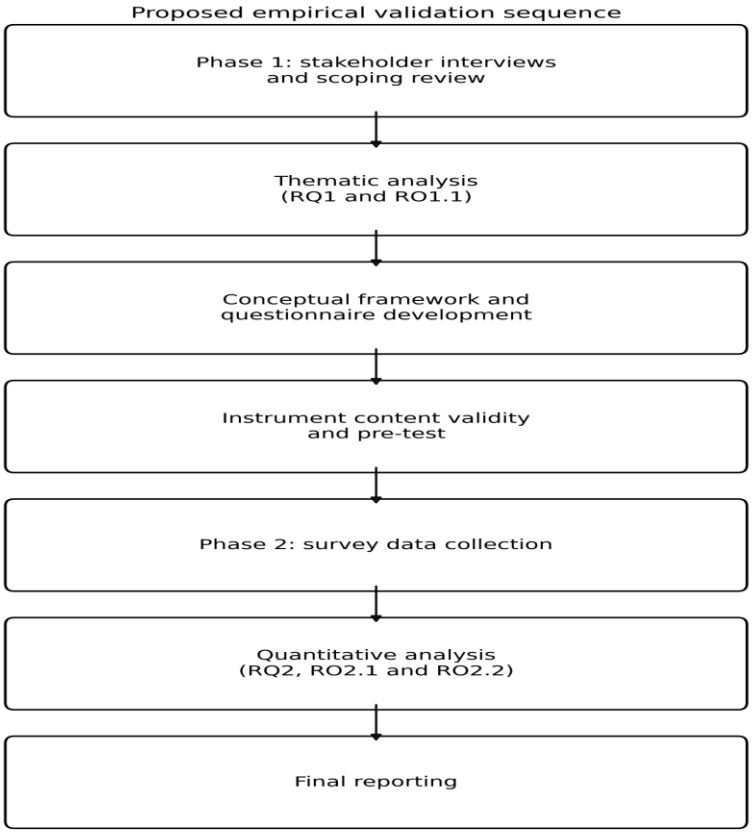
The final sample size would be determined through a priori power analysis after the framework and measurement model are finalized; the current plan anticipates at least 200 participants as an initial recruitment target, subject to the power needed to detect the four moderation effects. Descriptive and preliminary analyses would be conducted in SPSS, followed by PLS-SEM in SmartPLS 4 to assess reliability, convergent and discriminant validity, and the hypothesized structural relationships. The four moderation hypotheses will be tested using separate privacy risk × persuasion-function interaction terms, with bootstrapped confidence intervals and simple-slope plots used to interpret any interactions. Relevant background variables, including age, digital literacy and previous mobile-health experience, will be considered when assessing the model. Figure 2 summarizes the proposed sequence.

The proposed purposive sample covers smartphone users in selected urban and semi-urban parts of central Malaysia. It may therefore underrepresent rural older adults, people who do not use smartphones and those who need substantial assistance with digital services. The eventual findings should not be generalized to all older adults in Malaysia without further sampling and testing.

Table 3: Proposed empirical validation plan

Phase	Participants and data	Purpose	Proposed analysis and output
Phase 1: preliminary qualitative study	Interviews with approximately three to five stakeholders from Malaysian health and cybersecurity organizations; brief questionnaire checks with older adults	Identify factors contributing to willingness or reluctance and assess the need for contextual refinement	Thematic review of stakeholder feedback; older-adult cognitive pre-testing; refine construct wording and questionnaire
Phase 2: quantitative model testing	Adults aged 60 years or older who use smartphones in selected urban and semi-urban locations in central Malaysia; an initial target of at least 200, subject to moderation power analysis	Examine disclosure factors and the four proposed moderating effects	SPSS descriptive analyses; PLS-SEM measurement and structural assessment; bootstrapped tests of four interaction terms and simple slopes

Figure 2: Proposed empirical validation flow



Note: Instrument pre-testing includes feedback from older adults on question wording and the disclosure scenario. Sample-size planning will take account of the four proposed interaction tests before the quantitative phase.

4. Policy and Ethical Implications

The proposed model has policy relevance because digital-health transformation depends on both technological capability and public willingness to participate. A privacy-aware model can help policymakers and system developers identify where disclosure reluctance is associated with perceived risk, insufficient benefit, low trust or the design of the disclosure process. In Malaysia, this perspective is relevant to efforts to expand digital healthcare while maintaining data privacy, patient safety and inclusive access.

Persuasive design requires particular ethical attention when services are intended for older adults. Reminders, prompts, defaults and explanations can support informed decision-making, but they should not undermine autonomy or pressure users to disclose more information than intended. Opaque consent processes, pre-selected options or emotionally manipulative messages can exploit limited digital literacy or excessive trust in authority. Privacy-by-design, transparent consent and accessible privacy information should therefore be treated as safeguards rather than optional interface features.

In practice, an application could explain in plain language why each item of health information is requested, who may access it and how long it will be kept. Optional data-sharing choices could be left unticked, with a clear way to decline or withdraw consent without misleading warnings or unnecessary loss of essential care. Large text, readable consent summaries and optional assistance from a trusted caregiver could help users make the decision themselves. These measures illustrate persuasion that supports understanding and control rather than pushing users towards disclosure.

The framework also emphasizes that inclusion is not achieved simply by increasing the number of digital services. Systems must make benefits understandable, reduce unnecessary disclosure, provide meaningful choices and communicate privacy protections in a way that older adults can evaluate. This approach links individual disclosure decisions with wider questions of digital trust, digital literacy and equitable participation in digital healthcare.

5. Conclusion

This conceptual paper develops a privacy trade-off model for older adults' personal health-information disclosure in Malaysia. The model combines privacy calculus theory with cognitive dissonance theory to explain how perceived privacy risk and perceived benefit shape disclosure willingness and how four persuasion paradigms may alter these relationships. It also positions information sensitivity, trust, service availability, critical mass, compatibility and complementarity as antecedents within the trade-off process.

The model contributes to gerontechnology and digital-health research by treating privacy disclosure as both a technology-adoption issue and a behavioral governance issue. Its practical value lies in directing attention to the conditions under which older adults may consider digital-health disclosure acceptable, including credible privacy protection, meaningful benefits, trustworthy platforms and non-coercive communication. These conditions are relevant to the design of inclusive digital health services and to broader debates on trust, security, privacy and the social consequences of digital transformation.

Once empirically examined, the framework can also help identify which barriers require more focused intervention and where resources should be directed to improve digital-health participation. Evidence on the relative importance of privacy risk, perceived benefit, trust, and persuasion conditions could support more specific strategies for system design and communication. This maintains the original study's practical objective of helping decision makers use evidence to address barriers to EHR and mobile-health adoption among older adults.

The framework remains conceptual and therefore requires empirical validation. The proposed two-phase design provides a route for contextual refinement and subsequent hypothesis testing. Future empirical work should also examine whether the four persuasion paradigms operate as expected among different groups of older adults and whether their effects vary according to digital literacy, experience with health applications

and the sensitivity of the information requested. The central ethical requirement is that persuasion should support informed choice rather than weaken it.

By distinguishing stated willingness from actual disclosure and by specifying the four interaction mechanisms, the framework offers testable explanations for when privacy concerns may have a stronger or weaker influence on older adults' decisions. Whether those explanations hold in practice, particularly outside smartphone-using urban and semi-urban groups, remains an empirical question.

Acknowledgement: This work was supported by the Research Management Centre, UiTM (UiTMSEL-DUCS) 2025 – DUCS-A, 600-UiTMSEL (PI.6/4/8)(009/2025).

Disclosure of generative AI use: OpenAI ChatGPT was used during manuscript preparation and revision to assist with language editing, clarity, organisation and suggestions for explaining the proposed model, measurement plan, and reviewer-requested changes. The authors retain responsibility for checking the references, reviewing the suggested revisions and approving the theoretical arguments, hypotheses and final text before submission. No empirical data or research findings were generated using AI. This disclosure is provided in accordance with the Information Management and Business Review author guidance on generative AI use.

References

Alanazi, H. O., Zaidan, A. A., Zaidan, B. B., Mat Kiah, M. L., & Al-Bakri, S. H. (2015). Meeting the security requirements of electronic medical records in the era of high-speed computing. *Journal of Medical Systems*, *39*(1), Article 165. https://doi.org/10.1007/s10916-014-0165-3

Amadea, A., & Indrawati. (2022). The influence of perceived usefulness, perceived ease of use, social influence, facilities conditions, lifestyle compatibility, and perceived trust on intention to use e-wallet Dana. *The International Journal of Business & Management*, *10*(8), 1–11. https://doi.org/10.24940/theijbm/2022/v10/i8/bm2208-002

An, J., Wan, K., Xiang, Z., Zhu, X., An, J., & Yang, Y. (2025). Effects of privacy concerns on older adults' discontinuous usage intention: The chain mediating effect of technology anxiety and the moderating role of perceived price value. *Frontiers in Public Health*, *13*, Article 1543409. https://doi.org/10.3389/fpubh.2025.1543409

Boise, L., Wild, K., Mattek, N., Ruhl, M., Dodge, H., & Kaye, J. (2013). Willingness of older adults to share data and privacy concerns after exposure to unobtrusive in-home monitoring. *Gerontechnology*, *11*(3), 428–435. https://doi.org/10.4017/gt.2013.11.3.001.00

Brehm, J. W. (1956). Post-decision changes in the desirability of alternatives. *Journal of Abnormal and Social Psychology*, *52*(3), 384–389. https://doi.org/10.1037/h0041006

Burger, J. M. (1999). The foot-in-the-door compliance procedure: A multiple-process analysis and review. *Personality and Social Psychology Review*, *3*(4), 303–325. https://doi.org/10.1207/s15327957pspr0304_2

Centola, D., Becker, J., Brackbill, D., & Baronchelli, A. (2018). Experimental evidence for tipping points in social convention. *Science*, *360*(6393), 1116–1119. https://doi.org/10.1126/science.aas8827

Cooper, J. (2019). Cognitive dissonance: Where we've been and where we're going. *International Review of Social Psychology*, *32*(1), Article 7. https://doi.org/10.5334/irsp.277

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford University Press.

Ford, E. W., Menachemi, N., Peterson, L. T., & Huerta, T. R. (2009). Resistance is futile: But it is slowing the pace of EHR adoption nonetheless. *Journal of the American Medical Informatics Association*, *16*(3), 274–281. https://doi.org/10.1197/jamia.M3042

Gauld, C., Watson, B., Lewis, I., White, K. M., & Pammer, K. (2021). An exploration of the effectiveness of in-person and online versions of the induced hypocrisy paradigm to reduce smartphone use among young drivers. *Transportation Research Part F: Traffic Psychology and Behavior*, *82*, 462–474. https://doi.org/10.1016/j.trf.2021.09.015

Halicka, K., & Surel, D. (2021). Gerontechnology—new opportunities in the service of older adults. *Engineering Management in Production and Services*, *13*(3), 114–126. https://doi.org/10.2478/emj-2021-0025

Hall, J. L., & McGraw, D. (2014). For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Affairs*, *33*(2), 216–221. https://doi.org/10.1377/hlthaff.2013.0997

Harmon-Jones, E., & Mills, J. (Eds.). (1999). *Cognitive dissonance: Progress on a pivotal theory in social psychology*. American Psychological Association.

Highfill, T. (2019). Do hospitals with electronic health records have lower costs? A systematic review and meta-analysis. *International Journal of Healthcare Management*, *13*(1), 65–71. https://doi.org/10.1080/20479700.2019.1616895

Huang, G., & Oteng, S. A. (2023). Gerontechnology for better elderly care and life quality: A systematic literature review. *European Journal of Ageing*, *20*(1), Article 27. https://doi.org/10.1007/s10433-023-00776-9

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Kisekka, V., & Giboney, J. S. (2018). The effectiveness of health care information technologies: Evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. *Journal of Medical Internet Research*, *20*(4), Article e107. https://doi.org/10.2196/jmir.9014

Kruse, C. S., & Beane, A. (2018). Health information technology continues to show positive effect on medical outcomes: Systematic review. *Journal of Medical Internet Research*, *20*(2), Article e41. https://doi.org/10.2196/jmir.8793

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for electronic health records. *Journal of Medical Systems*, *41*(8), Article 127. https://doi.org/10.1007/s10916-017-0778-4

Malarvizhi, C. A. N., Al Mamun, A., Reza, M. N. H., & Masud, M. M. (2024). Ageing well with tech: Exploring the determinants of e-healthcare services adoption in an emerging economy. *Digital Health*, *10*, Article 20552076241272577. https://doi.org/10.1177/20552076241272577

McGrath, A. (2017). Dealing with dissonance: A review of cognitive dissonance reduction. *Social and Personality Psychology Compass*, *11*(12), Article e12362. https://doi.org/10.1111/spc3.12362

Ministry of Health Malaysia. (2016). *Malaysian Health Data Warehouse (MyHDW)*. https://www.moh.gov.my/moh/resources/Penerbitan/Portofolio/MyHDW_Brochure.pdf

Nguyen, L., Bellucci, E., & Nguyen, L. T. (2014). Electronic health records implementation: An evaluation of information system impact and contingency factors. *International Journal of Medical Informatics*, *83*(11), 779–796. https://doi.org/10.1016/j.ijmedinf.2014.06.011

Nilashi, M., Ahmadi, H., Ahani, A., Ravangard, R., & Ibrahim, O. B. (2016). Determining the importance of hospital information system adoption factors using fuzzy analytic network process (ANP). *Technological Forecasting and Social Change*, *111*, 244–264. https://doi.org/10.1016/j.techfore.2016.07.008

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of the healthcare sector: A study on privacy and security concerns. *ICT Express*, *9*(4), 571–588. https://doi.org/10.1016/j.icte.2023.02.007

Politi, L., Codish, S., Sagy, I., & Fink, L. (2022). Substitution and complementarity in the use of health information exchange and electronic medical records. *European Journal of Information Systems*, *31*(2), 188–206. https://doi.org/10.1080/0960085X.2020.1850185

Risen, J. L., & Chen, M. K. (2010). How to study choice-induced attitude change: Strategies for fixing the free-choice paradigm. *Social and Personality Psychology Compass*, *4*(12), 1151–1164. https://doi.org/10.1111/j.1751-9004.2010.00323.x

Robinson, S. C. (2018). Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 214–233. https://doi.org/10.1080/10919392.2018.1482601

Rothstein, M. A. (2007). Health privacy in the electronic age. *Journal of Legal Medicine*, *28*(4), 487–501. https://doi.org/10.1080/01947640701732148

Sittig, D. F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Quality and Safety in Health Care*, *19*(Suppl. 3), i68–i74. https://doi.org/10.1136/qshc.2010.042085

Sun, S., Jiang, L., & Zhou, Y. (2024). Associations between perceived usefulness and willingness to use smart healthcare devices among Chinese older adults: The multiple mediating effect of technology interactivity and technology anxiety. *Digital Health*, *10*, 20552076241254194. https://doi.org/10.1177/20552076241254194

Sun, Z., Pan, G., Yang, R., Zang, G., & Zhou, J. (2026). Consumer privacy decision-making in the digital era: An integrative review and taxonomy. *Aslib Journal of Information Management*, *78*(2), 307–335. https://doi.org/10.1108/ajim-12-2023-0526

Verheij, R. A., Curcin, V., Delaney, B. C., & McGilchrist, M. M. (2018). Possible sources of bias in primary care electronic health record data use and reuse. *Journal of Medical Internet Research*, *20*(5), Article e185. https://doi.org/10.2196/jmir.9134

Wang, Y., Kung, L., & Byrd, T. A. (2018). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting and Social Change*, *126*, 3–13. https://doi.org/10.1016/j.techfore.2015.12.019

Yan, Y., & Xing, H. (2025). Technology for sustainable living: The impact of digital inclusion on the health of China's elderly living alone. *SSM-Population Health*, *29*, Article 101751. https://doi.org/10.1016/j.ssmph.2025.101751