12-7-2022

# A Compliance-Based Framework for Digital Identity Management

Lillian Peiwen Li
*RMIT University*, s3232035@student.rmit.edu.au

Hepu Deng
*RMIT University*, hepu.deng@rmit.edu.au

Sophia Duan
*RMIT University*, sophia.duan2@rmit.edu.au

# A Compliance-Based Framework for Digital Identity Management

## Research-in-progress

**Lillian Peiwen Li**
School of Accounting, Information Systems and Supply Chain
RMIT University
Melbourne, Australia
Email: s3232035@student.rmit.edu.au

**Hepu Deng**
School of Accounting, Information Systems and Supply Chain
RMIT University
Melbourne, Australia
Email: hepu.deng@rmit.edu.au

**Sophia Duan**
School of Accounting, Information Systems and Supply Chain
RMIT University
Melbourne, Australia
Email: sophia.duan2@rmit.edu.au

## Abstract

Managing the digital identity is critical for minimizing the potential loss from identity theft in organizations. How digital identity can be better managed, however, remains to be addressed. This study investigates what affects the adoption of a compliance-based approach for managing digital identities in organizations. A comprehensive review of the related literature has been conducted, leading to the development of a compliance-based framework by integrating the unified theory of acceptance and use of technology and the general deterrence theory for better understanding the adoption of the compliance-based approach. This framework can then be tested and validated using structural equation modelling of the survey data collected, leading to the identification of the critical factors affecting the adoption of the compliance-based approach to manage digital identities. It contributes to existing digital identity management literature by proposing an integrated framework for better exploring the adoption of a compliance-based approach for managing digital identities.

**Keywords:** Digital identity, critical factors, compliance, technology adoption.

# 1 Introduction

Managing digital identities which are the digital representation of identifiable information of individuals in information systems (Gangire et al. 2019) is becoming increasingly important due to the potential misuse of such information with profound consequences (AlKalbani et al. 2019). Australian Competition and Consumer Commission (2020) shows that more than $3.5 billion has been lost due to digital identity breach from 2015 to 2020. Gangire et al. (2019) state that digital identity breach has reached at the epidemic level with identities being stolen at almost 500 a day. Adequately managing digital identities in organizations is therefore becoming critical.

There are various approaches for managing digital identities from the perspective of technologies, organizations, and individuals (AlKalbani et al. 2019). Technology-based approaches focus on using appropriate technologies to manage digital identities (Gangire et al. 2019). Organization-oriented approaches concentrate on developing specific strategies and policies for digital identity management (Sommestad et al. 2016). Individual-aligned approaches explore the behavior and attitude of individuals in protecting digital identities (AlKalbani et al. 2019). With the increasing use of digital technologies and the growing awareness of the importance of digital identities, the adoption of compliance-based approaches has become popular for digital identity management (Sommestad et al. 2016). In this context, a compliance-based approach is referred to as the process of monitoring and assessing organizational systems and processes to ensure that individuals mandatorily follow the strategies, policies, and standards in managing digital identities in organizations (Safa et al. 2019).

There are several studies on the adoption of compliance-based approaches for managing digital identities. Sommestad et al. (2016) demonstrate that adopting compliance-based approaches can better protect digital identities. AlKalbani et al. (2019) show that the adoption of compliance-based approaches can increase individuals' adherence to organizational policies and processes for safeguarding digital identities. Wu et al. (2021) discover that implementing compliance-based approaches helps individuals comply with policies and standards in managing digital identities. These studies demonstrate that adopting compliance-based approaches plays a critical role in managing digital identities. There is, however, lack of comprehensive understanding of the adoption of compliance-based approaches in managing digital identities.

This study investigates what affects the adoption of compliance-based approaches for managing digital identities. A review of the related literature has been conducted, leading to the development of a compliance-based adoption framework for better understanding the adoption of compliance-based approaches. Such a framework can then be tested and validated, leading to the identification of the critical factors for affecting the adoption of the compliance-based approach.

# 2 Related Work

Adopting compliance-based approaches for managing digital identities is to ensure that individuals can follow organizational strategies, policies, and standards in accessing digital identities (AlKalbani et al. 2019). The effectiveness of such approaches is often influenced by the motivation of individuals, the commitment of management and the presence of deterrence (Sommestad et al. 2019).

The motivation of individuals directly affects their intentions to adopt compliance-based approaches for digital identity management (Koohang et al. 2019). Although organizations actively use advanced technologies to manage digital identities, all these efforts are in vain if employees are not motivated to comply to the policies and standards. Employees with negative attitudes can undermine the enforcement of digital identity management policies and standards (Hong and Furnell 2022).

Management commitment reflects the determination of organizations to compliance-based identity management (AlKalbani et al. 2019). Safeguarding digital identities is the responsibility of everybody in organizations. Management needs to be committed in providing adequate funding and support for digital identity management (Sommestad et al. 2019). Organizations that lack a solid commitment from management face an increased risk of identity theft (Hong and Furnell 2022).

The presence of deterrence is to minimize no-compliance behaviors (Sommestad et al. 2019). Deterrence helps preventing future offence by frightening the potential offenders with adversary impact (Trang and Brendel 2019). Nonetheless, deterrence alone is not effective in reducing identity breach.

Numerous studies have been conducted for understanding how organizations can better adopt the compliance-based approaches for managing digital identities. Such studies can be classified into three groups including motivation-based studies, behavior-oriented studies, and deterrence-focused studies.

Motivational-based studies focus on comprehending what motivates employees to adopt compliance-based approaches for managing digital identities (Hsu et al. 2015). Posey et al. (2013) reveal that self-efficacy, perceived threat severity, and perceived threat vulnerability have a substantial impact on employees' motivations of protective behaviors based on the protection motivational theory (PMT). Hsu et al. (2015) show that intrinsic motivation, shared norms and values, and social pressure play critical roles to drive desired behaviors in information security compliance from the social control theory (SCT) perspective. Feng et al (2019) demonstrate that intrinsic factors such as attachment, involvement, commitment, and personal belief can strengthen the social bond between employees and shape their motivations to comply with information security policies and standards based on the social bond theory (SBT). Gangire et al. (2021) state that competence, relatedness and autonomy positively influence their motivation to comply with information security policies and standards based on the self-determination theory (SDT). These studies have demonstrated that intrinsic motivation is critical for adopting compliance-based approaches in managing digital identities.

Behavior-oriented studies aim to understand what affects the behavior of individuals in adopting compliance-based approaches to manage digital identities. Sommestad et al. (2019) employ the theory of planned behavior (TPB) to evaluate security behaviors, indicating that attitude, subjective norms, and perceived behavioral control, habit and regret have substantial impact on information security compliance. Baral et al. (2019) study digital identity theft using the technology threat avoidance theory (TTAT) showing that self-efficacy, establishment of information security policies and standards, and risk tolerance are crucial for managing digital identities. Natasya et al. (2019) apply the unified theory of acceptance and use of technology (UTAUT) to analyze taxpayers' acceptance of e-filing systems and the compliance of taxpayers, revealing that performance expectancy, effort expectancy, social influence and facilitating conditions are critical for affecting compliance behavior.

Deterrence-focused studies concentrate on comprehending how sanction impacts employees' intentions to comply with information security policies and standards. Trang and Brendel (2019) apply the general deterrence theory (GDT) to understand how to prevent future offences, demonstrating that sanction severity and sanction certainty are the powerful determinants in frightening potential offenders. Safa et al. (2019) apply the situational crime prevention theory (SCPT) based model to mitigate insider threats on information security, suggesting that increased sanction severity and decreased incentives and provocations positively influence the intention to prevent information security mis-behavior. Wu et al. (2021) investigate patients' compliance behavior based on the rational choice theory (RCT), concluding that the cost and benefit of noncompliance are the compelling factors to foster the compliant mindset of individuals. Table 1 summarizes the discussion above.

| Studies | Theories | Critical factors | References |
|---|---|---|---|
| Motivation | PMT | Rewards, self-efficacy, perceived threat severity, and perceived threat vulnerability | Posey et al. (2013) |
| | SCT | Intrinsic motivation, shared norms and values, and social pressure | Hsu et al. (2015) |
| | SBT | Attachment, involvement, commitment, and personal belief | Feng et al. (2019) |
| | SDT | Individual autonomy, competence, relatedness | Gangire et al. (2021) |
| Behavior | TPB | Attitude, subjective norms, and perceived behavioral control, habit and regret, | Sommestad et al. (2019) |
| | TTAT | Self-efficacy, information security policies and standards, and risk tolerance | Baral et al. (2019) |
| | UTAUT | Performance expectancy, effort expectancy, social influence and facilitating conditions | Natasya et al. (2019) |
| Deterrence | GDT | Sanctions severity and sanction certainty | Trang and Brendel (2019) |
| | SCPT | Increased sanction and decreased incentives | Safa et al. (2019) |
| | RCT | Cost and benefit of noncompliance | Wu et al. (2021) |

*Table 1. Summary of studies on the adoption of compliance-based approaches*

Existing studies discussed above largely focus on exploring the adoption of compliance-based approaches for managing digital identities from different perspectives. There is, however, lack of comprehensive understanding of the adoption of compliance-based approaches in managing digital identities (Venkatesh et al. 2016; Moody et al. 2018). This drives the current study to address the extant research gap through integrating UTAUT and GDT in exploring the adoption of the compliance-based approach for digital identity management.

# 3 A Compliance-Based Framework

This study develops a conceptual framework based on the integration of UTAUT and GDT for better understanding the adoption of the compliance-based approach in managing digital identities. Managing digital identities using compliance-based approaches is fundamentally a technology adoption issue. UTAUT is adopted for exploring individuals' attitude towards technology adoption. It has been extensively empirically tested and proven to be effective to capture the commonalities between different theories that can be used to complement each other to explore individuals' attitude towards technology adoption. GDT is used for better understanding the impact of sanction mechanisms towards individuals' behavior in digital identity compliance (Trang and Brendel 2019). Such a theory has been validated for explaining the relationship between social responsiveness and compliance intention (Moody et al. 2018). The integration of these two theories provides a comprehensive theoretical foundation for better exploring the adoption of the compliance-based approach to digital identity management.

Within the integration of UTAUT and GDT, a conceptual framework is developed for understanding the adoption of a compliance-based approach to manage digital identities as shown in Figure 1. This framework brings together a moderated technology adoption model and a social-psychological model, which allows us to explain self-interest and altruistic motivations to adopt a compliance-based approach in digital identity management. The framework is reflected in six dimensions including performance expectancy, effort expectancy, social influence, facilitating conditions, sanction severity and sanction certainty sharing.

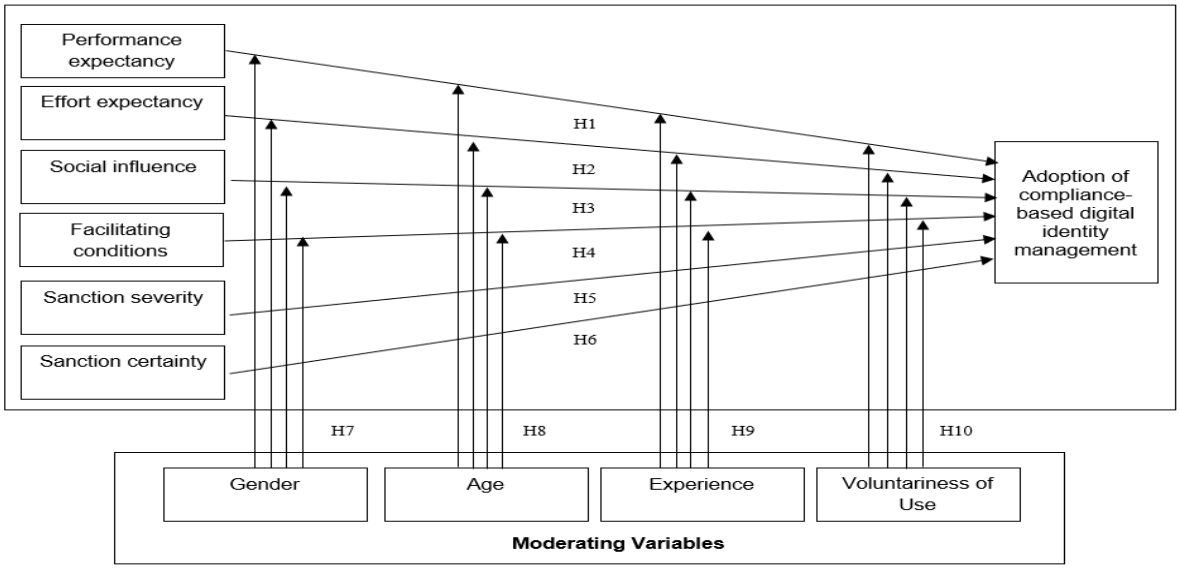


*Figure 1: Compliance-based Digital Identity Management Framework*

Performance expectancy is the degree to which individuals believe that using information technologies can help performing their work (Venkatesh et al. 2016). It is measured by how the use of digital technologies can help individual achieve digital identity compliance. The effect of performance expectancy for achieving digital identity compliance has been explored (Baral et al. 2019; Safa et al. 2019; Wu et al. 2021). Baral et al. (2019) find that the reliability of the technology has a direct influence on the individual's intention to utilise the technology. Safa et al. (2019) demonstrate that technology compatibility is critical for successful management of digital identity. Wu et al. (2021) state that the compatibility of different security technologies can help to improve the overall security of the organization's technologies. Based on the discussed above, the following hypothesis is proposed:
*H1: Performance expectancy has a positive impact on the adoption of compliance-based approaches*

Effort expectancy is about individuals' perceived effort on the ease of use of information technologies (Venkatesh et al. 2016). Individuals who find that the technology is user-friendly tends to adopt the technology (Natasya et al. 2019). It is measured by the extent that the digital technology is easy for individuals to use in achieving digital identity compliance. Several studies have been conducted on the impact of effort expectancy on compliance behavior. Natasya et al. (2019) state that effort expectancy plays a significant role in influencing individuals' intention to comply with organizational requirements.

Safa et al. (2019) claim that easy-to-use technologies have a positive influence on the adoption. As a result, the following hypothesis has been proposed.
*H2: Effort expectancy has a positive impact on the adoption of compliance-based approaches.*

Social influence is about the degree to which individuals perceive that others important to them believe that they should use the technology (Venkatesh et al. 2016). This is measured by the extent that the family, friends or colleagues find that the use of digital technology can help achieve digital identity compliance. When individuals find that people that they trust have adopted specific technologies, they tend to consider the technology to be competent in protecting information (Hsu et al. 2015). A few studies have demonstrated the effect of social influence on digital identity compliance (Hsu et al. 2015; Natasya et al. 2019). Hsu et al. (2015) state that social influence has a positive effect on the adoption of mobile payment services. Natasya et al. (2019) find that social influence is positively associated with the adoption of a mobile payment system. In digital identity compliance, important people like friends, family members and colleagues may influence individuals' positive attitude towards information security for achieving digital identity compliance. The following hypothesis is then developed:
*H3: Social influence has a positive impact on the adoption of compliance-based approaches.*

Facilitating condition is the degree to which individuals believe that organizational infrastructure exists to support the use of technologies (Venkatesh et al. 2016). This is assessed by how existing organizational infrastructure can help individual achieve digital identity compliance. Facilitating condition considers both external and internal conditions for adopting a new technology. The external condition focuses on the availability of external resources for the adoption of the technology. The internal condition looks into the ability of individuals to adopt the technology (Hsu et al. 2015). Koohang et al. (2019) show that individual's training and awareness in information security has a direct influence on information security compliance. Hong and Furnell (2022) claim that the responsibility of digital identity management is a part of corporate governance, and top management must provide direction and commitment for the successful implementation of digital identity management. Thus, the following hypothesis is proposed:
*H4: Facilitating conditions have a positive impact on the adoption of compliance-based approaches.*

Sanction severity is about the perceived degree of punishment on the violation of information security policies (Hsu et al. 2015). This is measured by how severe the punishment is when individuals violate the digital identity compliance requirement. Individuals who realize the severity of the punishment for violation are more likely to adhere to information security policies and procedures (Treng and Brendel 2019). Previous studies have found that the implementation of formal sanctions is crucial for achieving effective information security compliance (Feng et al. 2019; Hsu et al. 2015; Treng and Brendel 2019). Hsu et al. (2015) point out that sanctions exert greater pressure on employees to follow information security practices for achieving digital identity compliance. Feng et al. (2019) claim that the organization needs to impose proper sanctions to employees for deviant behavior in achieving digital identity management compliance. Treng and Brendel (2019) show that the use of sanctions can facilitate a positive information security culture for achieving digital identity management compliance. As a result, the following hypothesis is proposed:
*H5: Sanction severity is positively related to the adoption of compliance-based approaches.*

Sanction certainty is about the detection of deviant behavior in the first place and the likelihood of the respective sanction being enforced (Treng and Brendel 2019). This is measured by how certain a punishment is to be imposed for not achieving digital identity compliance. The consistent use of sanctions to individuals with violation increases their likelihood to adhere to policies and procedures (Koohang et al. 2019). Previous studies have been conducted on the effect of sanction certainty on compliance behavior. Hsu et al. (2015) state that the certain sanction in information security has a direct influence on information security compliance. Koohang et al. (2019) find that certainty action is an important aspect of enforcement. Safa et al. (2019) point out that the certain use sanctions positively influence digital identity compliance. The following hypothesis is then developed:
*H6: Formal sanction certainty is positively related to the adoption of compliance-based approaches.*

Personal characteristics influence the relationship between the critical factors discussed above and the adoption of compliance-based approaches to digital identity management. Age, gender, social influence, and voluntariness of use can have an impact on the association between these variables and the use of compliance-based approaches. Karahanna et al. (1999) reveal that gender significantly moderates the association between performance expectancy, effort expectancy, social influence and facilitating conditions and the use of the compliance-based approach. Venkatesh et al. (2016) find that men's performance expectancy, which focuses on task completion, is likely to be higher, whereas women's

effort expectancy is higher, and therefore influence compliant behavior in managing digital identities. Wu et al. (2021) further state that women have sufficient experience with new technology to be less impacted by conformity processes and more likely to adopt a new solution voluntarily. Thus, the following hypotheses are proposed:
*H7a-7d: Gender moderates the relationship between performance expectancy, effort expectancy, social influence, facilitating conditions and the adoption of compliance-based approaches.*

Old users with varying capacities have difficulties following guidelines to deploy new information systems due to their age. They are found to struggle more to adapt to new instructions and comply to various guidelines and requirements. Venkatesh et al (2016) find that age moderates the effects of facilitating conditions on actual adoption behavior. Baral et al. (2019) state that the likelihood of success in introducing new products or services is strongly correlated with age and voluntariness to use such product or service. Therefore, the following hypotheses are developed:
*H8a-8d: Age moderates the relationship between performance expectancy, effort expectancy, social influence, facilitating conditions and the adoption of compliance-based approaches.*

Individuals' experience affects performance and effort expectancies, which influences the adoption of specific technologies (Venkatesh et al. 2016). Natasya et al. (2019) show that individuals who lack experience find it difficult to adopt a new technology. To explain the relationship between the key factors and the resulting compliant to digital identity management, the impact of experience must be taken into account as moderating factor (Koohang et al. 2019). Thus, the following hypotheses are developed:
*H9a-9d: Experience moderates the relationship between performance expectancy, effort expectancy, social influence, facilitating conditions and the adoption of compliance-based approaches.*

Voluntariness of use is the degree to which individuals see a choice between using and not using technologies (Venkatesh et al. 2016). It is critical for affecting the desire to comply with digital identity management. Karahanna et al. (1999) claim that voluntariness of use defines the strength of perceived performance and effort. Natasya et al. (2019) reveals voluntariness of use has a moderating effect on the relationship between social influence and behavioral intention in information security compliance. The following hypotheses are then proposed:
*H10a-10d: Voluntariness of use moderates the relationship between performance expectancy, effort expectancy, social influence, facilitating conditions and the adoption of compliance-based approaches.*

# 4 Methods and Contributions

This study develops a conceptual framework for better understanding the adoption of compliance-based approaches to digital identify management. A survey-based quantitative approach will be adopted in this study. The participants' opinions will be gauged using a five-point Likert scale. A minimum sample of 200 participants will be obtained for this study. The survey participants will be employees of the selected Australian organizations who own digital identities or have previous experience in handling digital identities. The collected data will be analysed using structured equation modelling.

This research intends to extend the existing adoption intention model to account for comprehensive social influences and include additional constructs and moderators to further the boundary conditions of the theories to facilitate the management of digital identities. Theoretically, it contributes to the digital identity management literature by integrating UTAUT and GDT to explain the adoption of the compliance-based digital identity management. This study serves as a springboard for future investigation and offers a helpful lens through which to examine influence of the identified factors on employees' adoption intentions toward complying with information security controls in broader contexts. Practically, the findings of this study offer a basis to formulate targeted strategies and policies for organizations to promote better management of digital identities in their pursuit of mandating information security practices in organizations.

# 5 Conclusion

This study analyses the critical factors for employees' adoption of the compliance-based approach to managing digital identities in organizations. This leads to the formation of a conceptual framework for investigating the critical factors critically affecting the compliance-based digital identity management. Such a framework offers a helpful lens through which to examine influence of the identified factors on employees' adoption intentions toward complying with digital identity management controls in broader contexts under varying conditions.

## References

Alkalnani, A., Deng, H., and Kam, B. 2019. "The influence of organizational enforcement on the attitudes of employees towards information security compliance," *Proceedings of the International Conference on Information and Communication Systems*, June 11-13, Irbid, Jordan.

Australian Competition and Consumer Commission, 2020, Digital platform inquiry, Retrieved from: https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.

Baral, G., Asanka, N., and Arachchilage, G. 2019. "Building confidence not to be phished through a gamified approach: conceptualising user's self-efficacy in phishing," *Proceedings of the 2019 Cybersecurity and Cyberforensics Conference*, DOI: 10.1109/CCC.2019.000-1.

Feng, G., Zhu, J., Wang, N., and Liang, H. 2019. "'How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond," *Journal of the Association for Information Systems* (20), pp. 2-17.

Gangire, Y., Da Veiga, A. and Herselman, M., 2019. "A conceptual model of information security compliant behaviour based on the self-determination theory," *Conference on Information Communications Technology and Society (ICTAS)* (pp. 1-6). IEEE.

Hong, Y., and Furnell, S. 2022. "Motivating information security policy compliance: Insights from perceived organizational formalization," *Journal of Computer Information Systems* (62:1), pp. 19-28.

Hsu, J. S., Shih, S. P., Hung, Y. W., and Lowry, P. B. 2015. "The role of extra-role behaviors and social controls in information security policy effectiveness," *Information Systems Research* (26), pp. 282-300.

Karahanna, E., Straub, D., and Chervany, N. 1999. "Information technology adoption across time: a cross-sectional comparison of pre- and post-adoption beliefs," *MIS Quarterly*, pp.183-213.

Koohang, A., Anderson, J., Nord, J. H., and Paliszkiewicz, J. 2019. "Building an awareness-centered information security policy compliance model," *Industrial Management & Data Systems* (120:1), pp. 231-247.

Moody, G.D., Siponen, M. and Pahnila, S., 2018. Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1).

Natasya, N., Tandililing, E. M., Angelus, M., and Kevin, K. 2019. "Tax E-filing system acceptance level on the taxation compliance: An application of the UTAUT approach," *The Winners* (20), pp. 33-47.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. "Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors," *MIS Quarterly*, pp. 1189-1210.

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M. and Sookhak, M. 2019. "Deterrence and prevention-based model to mitigate information security insider threats in organisations," *Future Generation Computer Systems* (97), pp.587-597.

Sommestad, T., Karlzén, H., and Hallberg, J. 2019. "The theory of planned behavior and information security policy compliance," *Journal of Computer Information Systems* (59), pp. 344-353.

Trang, S., and Brendel, B. 2019. "A meta-analysis of deterrence theory in information security policy compliance research," *Information Systems Frontiers* (21), pp. 1265-1284.

Venkatesh, V., Thong, J. Y., and Xu, X. 2016. "Unified theory of acceptance and use of technology: A synthesis and the road ahead," *Journal of the Association for Information Systems* (17), pp. 328-376.

Wu, D., Lowry, P. B., Zhang, D., and Parks, R. F. 2021, "Patients' compliance behavior in a personalized mobile patient education system (PMPES) setting: Rational, social, or personal choices?" *International Journal of Medical Informatics* (145), 104