XXIV SEMEAD
Seminários em Administração
novembro de 2021
ISSN 2177-3866

INFORMAÇÕES DE SAÚDE EM CLOUD COMPUTING: ANALISANDO AS PREOCUPAÇÕES COM PRIVACIDADE NO USO DE APLICATIVOS MÓVEIS

HAMILTON OLIVEIRA
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO (FGV-EAESP)

CLÁUDIO LUÍS CARVALHO LARIEIRA
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO (FGV-EAESP)

ADILSON
UNIVERSIDADE PRESBITERIANA MACKENZIE (MACKENZIE)

INFORMAÇÕES DE SAÚDE EM *CLOUD COMPUTING*: ANALISANDO AS PREOCUPAÇÕES COM PRIVACIDADE NO USO DE APLICATIVOS MÓVEIS

1. Introdução

Há mais de uma década *Cloud Computing* (CC) fora indicado como um modelo tecnológico impulsionador da digitalização na indústria de saúde (Agarwal, Guodong, DesRoches e Jha, 2010), podendo ser definida como a entrega de recursos de Tecnologia da Informação (TI) como servidores, rede, bancos de dados (entre outros) sob demanda, por meio da *Internet* e com definição de preço e pagamento conforme o uso (Mell e Grance, 2011).

Ao considerar como as tecnologias podem mudar a maneira de se comunicar em saúde, pesquisadores identificaram o crescente interesse em plataformas de gerenciamento de informações centradas no paciente (Agarwal *et al.*, 2010) (Yaraghi, Gopal e Ramesh, 2019). Mobile Health (m-Health), a tecnologia que usa aplicativos em dispositivos móveis para habilitar a troca de informações de saúde, se tornou um novo canal em substituição ao tratamento de saúde presencial, sendo capaz de simplificar o cuidado com saúde e pesquisa médica e revolucionar a maneira pela qual indivíduos interagem com seus médicos, clínicas, laboratórios e outros provedores de saúde (Liwei, Baird e Rai, 2019).

Ao se estabelecer como uma plataforma multilateral (Sambamurthy e Zmud, 2017) (Shapiro, Shapiro e Varian, 1998), os m-Health centralizariam um grande volume de informações de saúde, e por ser em essência uma tecnologia centrada no indivíduo, as consequências negativas no caso de comprometimento das informações poderia afetar suas preocupações quanto à privacidade (Agarwal *et al.*, 2010). Experiências negativas no passado envolvendo privacidade também podem aumentar a resistência à assimilação de determinada tecnologia e intensificar as preocupações com relação a privacidade (Smith, Milberg e Burke, 1996).

Um importante desafio para a implementação de m-Health está relacionado à escolha da plataforma de saúde pelos indivíduos e sua integração com registros eletrônicos de saúde (EHR - *electronic health record*) (Gilbert e Cribbs, 2020). O EHR é uma estrutura baseada em computador para organizar e armazenar dados de saúde e contribui para facilitar o atendimento ao paciente, a colaboração do médico, melhora a qualidade e aumenta o valor do compartilhamento de informações na área da saúde (Angst e Agarwal, 2009) (Kohli e Tan, 2016).

Enquanto a digitalização no setor de saúde visa prover um melhor tratamento aos pacientes e é um tema discutido extensivamente desde a última década, ela traz consigo um tema controverso: a privacidade da informação (Agarwal *et al.*, 2010) (Anderson e Agarwal, 2011) (Angst e Agarwal, 2009). Estudos apontam que "o risco de acesso e disseminação não autorizados de informações de saúde digitalizadas e os riscos associados à privacidade do paciente tornaram-se uma das maiores preocupações associadas aos EHRs" (Kim e Kwon, 2019, p. 1185). Portanto, a capacidade de fornecer mecanismos para dar transparência e controle sobre as questões de privacidade para proteger adequadamente os dados pode ser o motivador para a divulgação de dados pelos indivíduos.

Assim, este estudo tem como objetivo investigar as preocupações dos indivíduos com relação a privacidade ao ter seus dados de saúde processados com m-Health, utilizando como referência conceitual o modelo MUIPC (*Mobile User's Information Privacy Concerns*) concebido por Xu, Gupta, Rosson e Carroll (2012). Foi utilizada a técnica de equações estruturais para avaliar a validade do modelo de mensuração bem como do modelo estrutural e os relacionamentos entre os construtos.

2. Fundamentação teórica

2.1. Privacidade da Informação

Privacidade da informação pode ser definida como a capacidade de dar controle ao indivíduo sobre suas informações pessoais (Smith *et al.*, 1996) para que possam determinar quando, como e com quem elas possam ser compartilhadas (Malhotra, Sung e Agarwal, 2004). Com o avanço da digitalização, as informações pessoais passaram a ser facilmente copiadas, transmitidas ou integradas, aumentando as ameaças relacionadas à privacidade (Malhotra *et al.*, 2004) a ponto de, para alguns autores, a privacidade da informação ser uma das questões éticas mais importantes da era da informação (Adjerid, Adler-Milstein e Angst, 2018) (Smith *et al.*, 1996).

Muitos estudos passaram a medir preocupações com privacidade como principal construto (Smith *et al.*, 1996) e, para isso, alguns modelos foram desenvolvidos. Por exemplo, Smith *et al.* (1996) elaboraram a escala *Concern for Information Privacy* (CFIP) que se aplica principalmente no estudo das preocupações dos indivíduos com privacidade na prática organizacional. Angst e Agarwal (2009) integraram ao CFIP o *Elaboration Likelihood model* para examinar a adoção de sistemas baseados em EHR. Malhotra *et al.* (2004) criaram a escala *Internet Users' Information Privacy Concerns* (IUIPC) que auxilia no estudo das preocupações com privacidade dos indivíduos que são usuários da *Internet*. A teoria proposta por Petronio (2002), denominada *Communication Privacy Management* (CPM), explica como os indivíduos gerenciam a divulgação ou encobrem suas informações privadas em diversos contextos, inclusive saúde.

Como diferentes tipos de informação pessoal, mecanismos de proteção, captura e finalidade de uso podem ter diferentes influências no comportamento do indivíduo na divulgação de suas informações, a principal dessas características são as preocupações com privacidade (Lin, Chen, Brown, Li e Yang, 2017). Sendo assim, o modelo escolhido para suportar este estudo é o MUIPC concebido por Xu *et al.* (2012) especialmente para examinar as preocupações com privacidade dos indivíduos no uso de dispositivos móveis. O modelo MUIPC será analisado com mais detalhes em seção futura neste artigo.

2.2. Privacidade da informação em saúde

EHR flexibiliza a integração dos dados de pacientes por estabelecer um padrão para a troca de informações entre diferentes sistemas computacionais de saúde, inclusive através da *Internet* (Kohli e Tan, 2016). Essa capacidade "facilita muito a disponibilidade de informações completas sobre a saúde do paciente" (Ozdemir, Barron e Bandyopadhyay, 2011, p. 491).

A ampla adoção de EHR viabilizou a troca de informações de saúde entre os diversos envolvidos no setor e essa possibilidade é hoje muito importante (Yaraghi *et al.*, 2019). No entanto, a interoperabilidade impulsionada pelo uso de EHR agrava as preocupações com privacidade. Pesquisa anterior já discutiu a relevância do tema "privacidade de informações de saúde" e as questões que surgiam estavam relacionadas à quanta informação precisa ser disponibilizada, como e para quem (Angst e Agarwal, 2009). Por facilitar a troca e distribuição das informações entre os diferentes interessados, EHR apresenta dificuldades em capturar e controlar o consentimento do paciente na divulgação e compartilhamento de suas informações (Angst e Agarwal, 2009) (Kim e Kwon, 2019) (Yaraghi *et al.*, 2019) (Yaraghi, Ye Du, Sharman, Gopal e Ramesh, 2015).

Fatores adicionais que implicam as preocupações com privacidade estão relacionados com a governança sobre os dados, propriedade, apropriação da informação e também envolvem os dispositivos que controlam a guarda, compartilhamento e manutenção da informação (Kohli e Tan, 2016). Outro componente agravante para as preocupações com a privacidade da

informação com o uso de EHR é a facilidade para transmitir informações de saúde através da *Internet* (Angst e Agarwal, 2009).

Estudos estimam que a unificação das informações de saúde em uma plataforma multilateral de informações de saúde (PMIS) pode reduzir em centenas de bilhões de dólares por ano as despesas com saúde (Adjerid *et al.*, 2018) (Ozdemir *et al.*, 2011) (Yaraghi *et al.*, 2019) (Yaraghi *et al.*, 2015). No entanto, os desafios para gerenciar e proteger a privacidade das informações dos pacientes são barreiras na expansão de uma PMIS (Yaraghi *et al.*, 2019). Para o uso e operacionalização de uma PMIS é necessário capturar o consentimento dos pacientes quanto ao uso de suas informações pessoais e de saúde (Yaraghi *et al.*, 2019) (Yaraghi *et al.*, 2015) . A capacidade de controlar o consentimento é resultado do desejo dos indivíduos por maior controle sobre suas informações, acentuado pelo aumento da preocupação com privacidade em razão do volume e natureza das informações envolvidas (Kohli e Tan, 2016).

Uma PMIS permite o acesso completo ao registro histórico do paciente para prover um tratamento de saúde mais apropriado, suporta as decisões médicas e direciona questões de saúde pública, minimizando tratamentos redundantes (Adjerid *et al*., 2018) (Kohli e Tan, 2016). Entretanto, restringir o acesso e controlar a privacidade das informações do paciente diante dos múltiplos envolvidos com distintos interesses são tópicos importantes e, por isso, desconsiderar esse tema comprometeria o sucesso e os potenciais benefícios trazidos por esta plataforma (Yaraghi *et al.*, 2019).

2.3. Cloud Computing e a privacidade da informação

A crescente adesão de CC na saúde pode reduzir custos com infraestrutura e operação de tecnologia computacional pela economia de escala (Gao e Sunyaev, 2019). A combinação do uso de CC e EHR é um estímulo à integração e interoperabilidade de informações de saúde (Ozdemir *et al.*, 2011), pois CC é uma tecnologia adequada para o compartilhamento de dados entre diferentes sistemas através da *Internet*, trazendo agilidade e flexibilidade, enquanto EHR é um modelo padrão definido para este tipo de dado (Ali *et al.*, 2018).

Várias ameaças, porém, são capazes de restringir a aceitação de CC em saúde. Algumas dessas ameaças são criptografia fraca, acesso público ao dado, vírus, *malwares*, além de questões relacionadas ao uso do dado (Ali *et al.*, 2018). Essas ameaças se relacionam com o fator determinante na adoção de CC em saúde: a preocupação com privacidade no tratamento de informações sensíveis. Se os indivíduos não confiarem que suas informações pessoais de saúde serão tratadas adequadamente, eles podem relutar em divulgar informações confidenciais ou sensíveis (Keil *et al.*, 2018).

Pesquisas indicam que as preocupações com privacidade das informações de saúde para uso com CC são um dos principais obstáculos a serem superados (Gao e Sunyaev, 2019) Sultan, 2014). Em seu estudo Kim e Kwon (2019) recomendam a implementação de certificados e diretivas na implementação de controles de privacidade no uso de EHR, o que desafia os prestadores e provedores de serviços em saúde a atender certos padrões relacionados a privacidade e segurança de dados.

A transação primária em uma plataforma m-Health é a informação de saúde do indivíduo que pode ser estruturado seguindo padrões EHR para facilitar o acesso e a interoperabilidade *(*Ozdemir *et al.*, 2011). Já o uso de CC flexibiliza a integração dos dados entre diferentes sistemas e partes interessadas, além de estimular a colaboração (Gao e Sunyaev, 2019). Essas características possibilitam que os m-Health atuem como um canal intermediário conectando indivíduos, prestadores, provedores e outros interessados na área de saúde.

A centralização de grandes volumes de informações de saúde com m-Health, onde a informação de saúde dos indivíduos da rede possa ser ativamente analisada, faz com que seja possível verificar, por exemplo, tendências de contágio, avanço de doenças e disparo de alertas

para partes interessadas (Sultan, 2014). No entanto, o volume de informações trafegada amplia os desafios relacionados com a privacidade de dados (Yaraghi *et al.*, 2019).

Juhee e Eric Johnson (2018) destacam os desafios relacionados à integração para compartilhamento de informações de saúde, as medidas de segurança de dados necessárias para isso e enfatizam o alto número de pacientes comprometidos com vazamento de dados. Uma plataforma que implemente o uso de EHR tem como consequência o armazenamento de uma grande quantidade de dados clínicos digitalizados transitando pela *Internet* e, na eventualidade de um comprometimento da plataforma, uma das principais consequências seria o prejuízo com a confidencialidade dos dados do paciente (Agarwal *et al.*, 2010).

Yaraghi *et al.* (2015) observaram que capturar o consentimento do paciente antes de que qualquer interessado possa acessar seus registros médicos pode reduzir as preocupações dos indivíduos quanto à privacidade das suas informações, pois estes passariam a ser informados de antemão sobre como seus dados serão tratados. Os dados de saúde pertencem aos pacientes e estes deveriam ter o poder de decidir como usar, com quem compartilhar e ter controle sobre seu dado (Sultan, 2014). Dar aos indivíduos controle sobre suas informações de saúde pode estimular positivamente a intenção de divulgação de dados entre interessados do setor e a adoção de determinada tecnologia (Yaraghi *et al.*, 2019).

Contudo, em uma plataforma composta por diversos interessados, pode ser difícil conseguir o acordo com todas as partes, consentindo com os termos que endereçam as preocupações dos indivíduos com privacidade e sejam aderentes às regulamentações focadas na proteção dos dados de saúde e outros dados sensíveis (Adjerid *et al.*, 2018). Essa combinação de fatores, contribuem para ampliar a importância do estudo sobre privacidade para uso de m-Health.

Por meio da análise desses estudos foi possível observar que a preocupação com privacidade é capaz de influenciar negativamente a intenção do indivíduo na divulgação de informações em tecnologias na indústria de saúde, seja no uso de EHR em uma plataforma multilateral de saúde ou no uso de CC (Angst e Agarwal, 2009) (Kim e Kwon, 2019) (Yaraghi *et al.*, 2019) (Yaraghi *et al.*, 2015), (Gao e Sunyaev, 2019) (Sultan, 2014), o que permite supor que o mesmo comportamento poderá se apresentar no uso de m-Health.

3. Modelo conceitual

O MUIPC (*Mobile User's Information Privacy Concerns*) é o modelo proposto por Xu *et al.* (2012) e foi desenhado exclusivamente para o estudo das preocupações com perda da privacidade no contexto do uso de dispositivos móveis. Esta escala, apresentada na Figura , está dividida em três dimensões de primeira ordem: vigilância percebida, intrusão percebida e uso secundário de informações pessoais.

Apesar de CC estar relacionado ao uso de recursos computacionais através da *Internet* (Mell e Grance, 2011) e a escala IUIPC ser desenhada especificamente para estudos concernentes às preocupações com privacidade através da *Internet* (Malhotra *et al.*, 2004), a inclusão do contexto de aplicativos móveis faz com que a escala MUIPC seja a mais adequada para este estudo. Além disso, estudos recentes se basearam nessa escala para examinar o efeito das preocupações com privacidade no uso de informações de bem-estar por dispositivos móveis (Vitak, Liao, Kumar, Zimmer e Kritikos, 2018), bem como do consentimento de permissões por aplicativos móveis (Degirmenci, 2020).

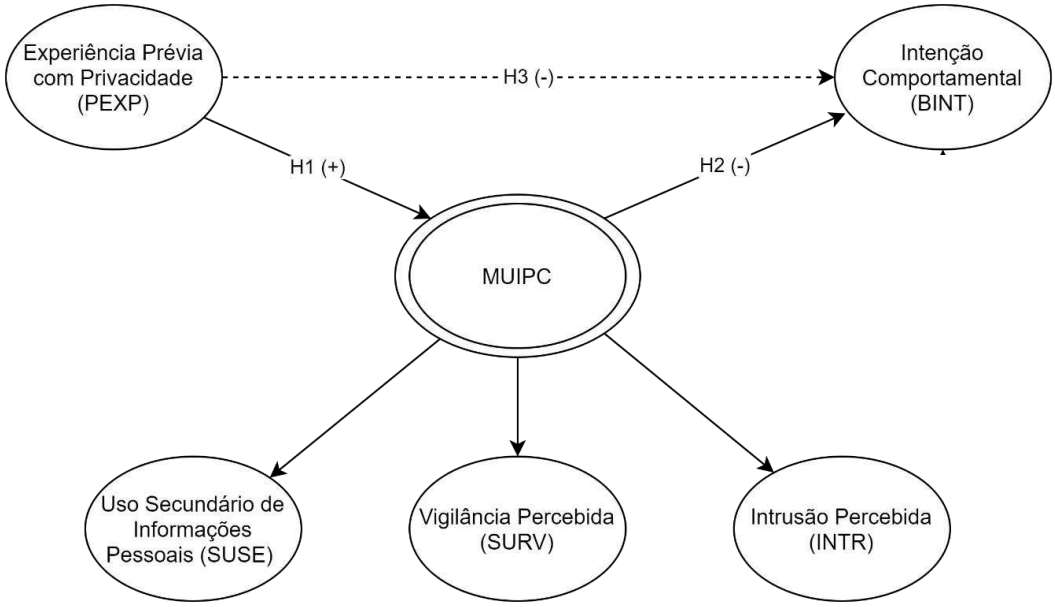

Figura 1 – Modelo MUIPC
Fonte: Adaptado de Xu *et al.* (2012).

Na escala proposta por Xu *et al.* (2012), MUIPC é o construto de maior ordem mensurado em um relacionamento reflexivo com os de menor ordem – vigilância percebida (SURV), intrusão percebida (INTR) e uso secundário de informações pessoais (SUSE) – que, por sua vez, são mensurados por indicadores reflexivos.

Vigilância percebida é descrita como o monitoramento e análise de perfil dos usuários de dispositivos móveis através do uso dos recursos tecnológicos embutidos e disponíveis (Xu *et al.*, 2012). A coleta de dados pelos dispositivos é o ponto de partida para as preocupações com privacidade (Malhotra *et al.*, 2004) e essa pode ser feita pelos sensores, câmeras, e os aplicativos presentes no dispositivo ou conectados a ele (Xu *et al.*, 2012). "Usuários de dispositivos móveis resistem aos aplicativos móveis por temer que suas atividades possam ser assistidas, gravadas e transmitidas a várias entidades" (Xu *et al.*, 2012, p. 4). Isso aconteceria se as informações integradas ao m-Health para visão única do estado de saúde dos indivíduos fossem divulgadas através da CC para uso impróprio.

Intrusão é a invasão do espaço pessoal do indivíduo que pode perturbar sua rotina ou solidão causando-lhe desconforto (Solove, 2006). Ela está relacionada ao uso não autorizado ou malicioso da informação pelo destinatário, que pode tirar proveito desse acesso para uso indevido das informações (Xu *et al.*, 2012). Pelo fato de os m-Health armazenarem e processarem informações sensíveis e, em alguns casos, confidenciais, se estas informações forem acessadas por outros aplicativos indevidamente, os usuários podem criar resistência para novos compartilhamentos em função deste acesso indesejado.

O uso secundário de informações pessoais é a coleta das informações dos indivíduos para uma finalidade diferente da inicialmente autorizada (Smith *et al.*, 1996). No caso de m-Health, o uso secundário de informações pessoais está ligado, por exemplo, ao uso promocional das informações de saúde dos indivíduos ou para fins de análise de perfil de saúde, sem seu consentimento. Essa situação pode ser considerada vazamento de informações, criando uma sensação de vulnerabilidade e falta de controle (Xu *et al.*, 2012).

Xu *et al.* (2012) validaram o construto MUIPC ao posicioná-lo mediando dois outros construtos: experiência prévia com violação de privacidade e intenção comportamental.

Experiência prévia com violação de privacidade (PEXP) é descrita como a exposição ou invasão da privacidade que resultaria em mal uso dos dados do indivíduo que, como consequência, teria fortes preocupações com a privacidade de seus dados (Smith *et al.*, 1996).

Malhotra *et al.* (2004) definem intenção comportamental (BINT) como a disposição do indivíduo em fornecer informações pessoais em determinado meio. Se refere a probabilidade de uma pessoa se comportar de uma forma específica ao utilizar determinada tecnologia. Na área de saúde foi um construto usado para medir aspectos do comportamento que relacionam a adoção e uso de determinada tecnologia que envolvem divulgação de dados pessoais (Angst e Agarwal, 2009) e, no contexto dessa pesquisa, a mesma definição se aplica, pois essa se refere a disposição do indivíduo em adotar ou usar m-Health e divulgar suas informações pessoais de saúde.

Ainda que Xu *et al.* (2012) tenham testado o modelo MUIPC para entender as preocupações com privacidade de usuários de aplicativos móveis e Silva Junior (2015) e Silva Junior, Luciano e Lübeck (2020) tenham testado essa escala no contexto brasileiro, esse estudo se propõe também a averiguar a aderência da escala para o uso de aplicativos móveis que utilizem CC como uma segunda camada tecnológica.

Através da escala MUIPC, esse estudo pretende endereçar a pergunta de pesquisa que tem como propósito investigar as preocupações com privacidade no uso de m-Health, analisando os construtos de primeira ordem da escala MUIPC – vigilância percebida, intrusão percebida e uso secundário de informações pessoais (Xu *et al.*, 2012). Xu *et al.* (2012) também propõem MUIPC como mediador dos construtos entre segunda ordem experiência prévia com privacidade (Smith *et al.*, 1996) e intenção comportamental, ou intenção de divulgação de informações pessoais (Malhotra *et al.*, 2004).

Como fundamentado na análise teórica, o grande número de dados trafegando pela *Internet* incrementa o risco de exposição das informações dos indivíduos e, se por uma experiência negativa com privacidade no passado esses não confiarem que suas informações pessoais de saúde serão tratadas adequadamente, eles podem relutar em divulgar informações confidenciais ou sensíveis (Keil *et al.*, 2018) e indivíduos expostos a violação de privacidade no passado apresentam maiores preocupações com privacidade por temerem o mal uso de suas informações pessoais (Smith *et al.*, 1996). Assim, foi proposta a **hipótese H1: Experiência anterior com violação de privacidade influencia positivamente as preocupações com privacidade da informação no uso de m-Health**.

Estudos anteriores na área de sistemas de informação já explicaram o efeito negativo das preocupações com privacidade na intenção comportamental para divulgação de informações pessoais dos indivíduos (Adjerid *et al.*, 2018) (Smith *et al.*, 1996) (Xu *et al.*, 2012), inclusive relacionados com saúde (Anderson e Agarwal, 2011). Com base nessas evidências, pode-se presumir que as preocupações com privacidade também influenciam negativamente o uso de m-Health pelos indivíduos. O risco de acesso e disseminação não autorizados de informações de saúde e os riscos associados à privacidade do paciente são fatores preponderantes para tomada de decisão e para a adoção de uma plataforma de troca de dados de saúde (Anderson e Agarwal, 2011) (Angst e Agarwal, 2009) (Yaraghi *et al.*, 2019). Estima-se então que o aumento das preocupações de privacidade, eventualmente, pode levar a uma redução na disposição dos indivíduos em adotarem m-Health para divulgarem informações de saúde. A partir desse argumento, é proposta a **hipótese H2*:* Preocupações com privacidade da informação no uso de m-Health influenciam negativamente a intenção comportamental**.

Xu *et al.* (2012) posicionaram MUIPC como mediador entre experiência prévia com violação de privacidade com intenção comportamental. Indivíduos que foram vítimas de violação de suas informações pessoais tem fortes preocupações com privacidade e, por sua vez, maiores preocupações com privacidade aumentam a probabilidade de recusa da divulgação de

suas informações pessoais ou uso de soluções que as solicitam (Smith *et al.*, 1996). Com o objetivo de examinar este argumento, propõe-se a hipótese **H3: Preocupações com privacidade da informação no uso de m-Health mediam a relação entre experiência anterior com perda de privacidade e a intenção comportamental**.

4. Metodologia de pesquisa

Esta é uma pesquisa que usa uma abordagem quantitativa com uma estratégia de investigação de levantamento de seção cruzada, onde os dados foram coletados em um único intervalo de tempo que permite extrair uma descrição quantitativa ao estudar uma amostra de uma população (Creswell, 2012).

A escolha do algoritmo PLS-SEM se deve ao fato dessa técnica permitir simultaneamente testar a escala e estimar o modelo estrutural, além de ser adequada para modelos com uma amostra reduzida (Chin, Marcolin e Newsted, 2003). Os construtos estão alinhados com a escala definida por Xu *et al.* (2012), usando indicadores reflexivos, em uma escala reflexiva-reflexiva. Para responder cada um dos itens da escala MUIPC, usou-se a escala *Likert* com intervalo de 7 pontos, variando entre 1 (discordo totalmente) e 7 (concordo totalmente). Esse intervalo foi escolhido para alcançar maior precisão quanto a percepção do respondente para cada item avaliado, limitando a ocorrência de variações significativamente altas ou baixas nos dados.

O aplicativo *SmartPLS* versão 3.3.2 foi usado neste estudo como ferramenta para analisar os resultados, validar empiricamente as hipóteses levantadas e a escala escolhida (MUIPC). Usando as capacidades desta ferramenta, primeiro foi avaliada a confiabilidade e validade do modelo, antes de se testar o modelo estrutural.

Devido à estratégia de investigação, optou-se pela coleta de dados através de uma *Survey*, pois esta técnica de coleta consegue explicar as razões e fontes de eventos, características e correlações observadas e facilita a aplicação cuidadosa do pensamento lógico, além de ser empiricamente verificável (Babbie, 1999). Como o objetivo principal desse estudo é examinar a preocupação dos indivíduos com privacidade no uso de m-Health, o questionário apresentado também forneceu informação contextual sobre a função dos aplicativos de saúde, seu armazenamento na nuvem e as principais questões envolvidas com o intuito de compartilhar um entendimento comum sobre a questão principal.

Os respondentes, não necessariamente já deveriam ser usuários ativos de m-Health, pois a intenção comportamental faz parte do escopo da pesquisa. Antes da fase de coleta de dados foi necessária a tradução da escala desenvolvida por Xu *et al.* (2012) e, para tal, utilizou-se como referência a tradução realizada por Silva Junior (2015) e Silva Junior *et al.* (2020), que já haviam traduzido a escala MUIPC usando retrotradução, técnica usada para identificar erros de tradução (Malhotra, 2006).

O estudo procurou obter com clareza o consentimento dos respondentes, uma vez que a intenção era capturar informações pessoais e sensíveis com o fim de cumprir com questões éticas (Creswell, 2012). Além disso, assegurou-se que as informações compartilhadas seriam anônimas e confidenciais. Para evitar ambiguidade, a pesquisa apresentou definições claras dos conceitos envolvidos e seus objetivos, baseados na definição da literatura disponível (Ali *et al.*, 2018) (Mell e Grance, 2011) (Ozdemir *et al.*, 2011) (Yaraghi *et al.*, 2015) e a escala usada incluiu dimensões e itens bem estabelecidos.

O questionário construído usando a plataforma *Google Forms* e sua validade foram verificados com a submissão a um pré-teste para 20 estudantes de pós-graduação *strictu sensu* em agosto de 2020, escolhidos por conveniência. Ao final do pré-teste, apenas um ajuste em uma questão demográfica (Renda Familiar) foi recomendado (pois faltava um intervalo entre

os valores) e foi aceita. Entre setembro e outubro de 2020, o questionário foi publicado nas redes sociais *WhatsApp* e *LinkedIn*, resultando em uma amostra por conveniência, uma vez que os participantes voluntariamente decidiram participar da pesquisa (Creswell, 2012). Para coleta de dados foi utilizada também uma técnica amostragem não probabilística, resultado do uso da técnica amostragem bola de neve.

5. Resultados da pesquisa e análises

5.1. Sobre a amostra

Foram realizadas verificações de controle de qualidade e adequação da amostra para que pudessem ser identificadas respostas inválidas, ausentes, padrões de respostas suspeitas e valores discrepantes (*outliers*). Um total de 310 respostas foram capturadas pela pesquisa, mas após a execução dos procedimentos mencionados a seguir obteve-se 262 válidas. Devido a uma limitação da ferramenta de coleta, algumas respostas do mesmo indivíduo foram enviadas em duplicidade. Através da ferramenta IBM SPSS foi possível fazer comparação entre todos os atributos, detectar 37 duplicidades e eliminá-las da amostra. Foi aplicada também uma avaliação pelo cálculo da distância quadrada de Mahalanobis (Hair, Hult, Ringle e Sarstedt, 2017a) e, como resultado, foram encontrados e removidos 10 *outliers* multivariados.

Da amostra válida de 262 respondentes, a maioria dos indivíduos são do sexo masculino (62,60%) e 71,76% têm entre 26 e 44 anos de idade. A renda média familiar de 61,83% dos respondentes é superior a R$ 10.000,00 e 61,07% afirmaram possuir curso superior e já terem feito alguma pós-graduação, seja *stricto sensu* ou *lato sensu*. Apesar da tentativa de se alcançar várias regiões através da rede social, os respondentes são em sua maioria residentes no estado de São Paulo, correspondendo a 91,60% da amostra. O número de respondentes que mora fora do Brasil – 2,67% – foi maior que qualquer outro estado.

Foi identificado que 65,65% dos respondentes possuem um dispositivo iOS, contra 33,97% que possuem dispositivos que usam plataforma Android e apenas 0,38% que usam ambas as plataformas. Como o estudo visa analisar as preocupações com privacidade com m-Health, o objetivo de se coletar esta informação é garantir que a pesquisa não fique restrita a determinada plataforma móvel.

5.2. Sobre a escala MUIPC para m-Health

Para responder uma hipótese de pesquisa deve-se utilizar uma escala válida. Portanto, como objetivo específico desse trabalho está a validação do MUIPC para m-Health. O primeiro passo usado para validar o modelo foi analisar as cargas fatoriais (*outer loadings)* dos indicadores MUIPC pesquisados. A execução do algoritmo PLS-SEM convergiu após 7 interações, atingindo assim uma solução estável com poucas interações. Uma definição amplamente aceita é a de que baixas cargas fatoriais, isto é, abaixo de 0,70 são consideradas fracas (Hulland, 1999) e, portanto, deve-se examinar a possibilidade de eliminá-la do modelo. Com base nesta regra, a tabela 1 apresenta que o indicador SURV1 é candidato à eliminação já que apresenta um desajuste em relação à escala, similarmente ao que ocorreu em outros estudos (Degirmenci, Guhr e Breitner, 2013) (Silva Junior, 2015) (Silva Junior *et al.*, 2020), não estabelecendo assim validade convergente para este indicador. Já o indicador PEXP2 foi mantido, pois ele está no limite tolerável de 0,40 – 0,70.

Tabela 1 – Carga Fatorial MUIPC

Construtos	Indicadores	Carga Fatorial
Intenção Comportamental	BINT1	0,886
	BINT2	0,965
	BINT3	0,964
Intrusão Percebida	INTR1	0,916
	INTR2	0,938
	INTR3	0,904
Experiência Prévia	PEXP1	0,840
	PEXP2	0,636
	PEXP3	0,860
Vigilância Percebida	SURV1	0,157
	SURV2	0,963
	SURV3	0,959
Uso Secundário	SUSE1	0,947
	SUSE2	0,956
	SUSE3	0,941

Fonte: Elaborado pelos autores (2021).

Sem o indicador SURV1, o algoritmo PLS-SEM novamente convergiu após 7 interações. Utilizando o critério de Fornell-Larcker (apresentado na tabela 2) no qual a raiz quadrada de AVE – valores na diagonal, em negrito – deve ser maior que as correlações com os demais construtos, observou-se que há validade discriminante.

Tabela 2 – Resultados da Avaliação do Modelo MUIPC

Construto	1	2	3	4	5
1 - Intenção Comportamental (BINT)	**0,939**				
2 - Intrusão Percebida (INTR)	-0,294	**0,919**			
3 - Vigilância Percebida (SURV)	-0,279	0,790	**0,963**		
4 - Experiência Prévia (PEXP)	-0,033	0,245	0,169	**0,786**	
5 - Uso Secundário (SUSE)	-0,145	0,727	0,687	0,248	**0,948**
Confiabilidade Composta	0,957	0,943	0,963	0,826	0,964
Variância Média Extraída (AVE)	0,882	0,845	0,928	0,617	0,899

Fonte: Elaborado pelos autores (2021).

A seguir, optou-se por analisar a confiabilidade composta para demonstrar a consistência interna do modelo. Todos os construtos apresentaram valores acima do limite recomendado de 0,70 (Hair *et al.*, 2017a), confirmando a confiabilidade do modelo. Foi analisada também a Variância Média Extraída (AVE), cujo valor mínimo exigido é de 0,50 (Fornell e Larcker, 1981). Todos os construtos apresentaram valores acima do limite estabelecido, o que demonstra alto nível de validade convergente.

Tabela 3 – Critério de Cargas Cruzadas

Indicadores	Intenção Comportamental	Intrusão Percebida	Vigilância Percebida	Experiência Prévia	Uso Secundário
BINT1	**0,887**	-0,238	-0,209	-0,032	-0,091
BINT2	**0,965**	-0,272	-0,257	-0,015	-0,132
BINT3	**0,964**	-0,309	-0,305	-0,044	-0,172
INTR1	-0,233	**0,916**	0,749	0,259	0,621
INTR2	-0,260	**0,938**	0,746	0,230	0,717
INTR3	-0,320	**0,904**	0,682	0,187	0,665
SURV2	-0,263	0,769	**0,964**	0,152	0,662
SURV3	-0,275	0,753	**0,963**	0,174	0,662
PEXP1	0,006	0,171	0,134	**0,842**	0,176
PEXP2	-0,019	0,150	0,131	**0,633**	0,205
PEXP3	-0,057	0,245	0,134	**0,861**	0,202
SUSE1	-0,104	0,692	0,654	0,223	**0,947**
SUSE2	-0,160	0,691	0,673	0,280	**0,956**
SUSE3	-0,148	0,685	0,626	0,202	**0,941**

Fonte: Elaborado pelos autores (2021).

Também foram avaliados os critérios de cargas cruzadas (tabela 3) como técnica adicional para determinar a validade discriminante. Nesse caso, a validade discriminante é estabelecida quando a carga dos indicadores atribuídas a um construto é maior que as cargas cruzadas dos indicadores atribuídos aos demais construtos (Hair *et al.*, 2017a). Novamente, há evidências de validade discriminante para os indicadores reflexivos.

Tabela 4 – *Heterotrait-Monotrait ratio*

Construtos	BINT	INTR	SURV	PEXP	SUSE
BINT					
INTR	0,316				
SURV	0,295	0,862			
PEXP	0,05	0,308	0,216		
SUSE	0,149	0,785	0,736	0,311	

Fonte: Elaborado pelos autores (2021).

Há situações, porém, nas quais essas técnicas são ineficazes em medir a validade discriminante (Henseler, Ringle e Sarstedt, 2015) e, por isso, como medida de contorno, optou-se também por avaliar a técnica HTMT (*Heterotrait-Monotrait ratio*). Hair *et al.* (2017b) recomendam considerar valores inferiores ao limite de 0,85 para HTMT para confirmar a validade discriminante entre dois construtos reflexivos. Embora a tabela 4 apresente apenas um valor nesta relação acima do limite proposto, o valor está abaixo de 0,90, limite estabelecido por Henseler *et al.* (2015) para HTMT, confirmando então a validade discriminante do modelo.

5.3. Exame do modelo estrutural

Um exame do modelo estrutural também deve ser avaliado antes de qualquer afirmação. O coeficiente de determinação, também chamado de R^2, é uma medida de ajuste de um modelo estatístico linear generalizado e é a maneira mais comum de avaliar o modelo estrutural, onde valores entre 0 e 1 indicam maior exatidão preditiva. Hair *et al.* (2017a, p. 199) destaca que "é difícil prover uma regra para valores de coeficientes de determinação aceitáveis e esse depende da complexidade do modelo e da disciplina de pesquisa". Para este estudo, usaremos como referência a proposta de Cohen (1988), que considera valores de R^2 em 2%, 13% e 26% indicando respectivamente uma variância explicada pequena, média e grande. Sendo assim, o valor dos R^2 nos relacionamentos entre os construtos examinados é pequeno.

Usando as regras que definem os critérios para análise do tamanho do efeito (f^2), onde 0,02, 0,15 e 0,35 indicam respectivamente um fraco, médio e forte efeito do construto exógeno no endógeno (Hair *et al.*, 2017a), é possível afirmar o tamanho do efeito para todos os relacionamentos do modelo também ser pequeno. Após uma avaliação da relevância preditiva de Stone-Geisser (Q^2) observou-se valores acima de 0, indicando relevância preditiva em relação aos construtos endógenos (Hair *et al.*, 2017a). Todos estes resultados estão apresentados na tabela 6.

Tabela 6 – Tamanhos do Efeito, Coeficiente de Determinação e Relevância Preditiva

Relação estrutural	f^2	R^2	Q^2
PEXP → MUIPC	0,066	0,062	0,045
MUIPC → BINT PEXP → MUIPC → BINT	0,072	0,067	0,056

Fonte: Elaborado pelos autores (2021).

Para simplificar a visualização, a figura 2 apresenta um resumo da análise dos coeficientes estruturais padronizados, valor-t e coeficientes de determinação.

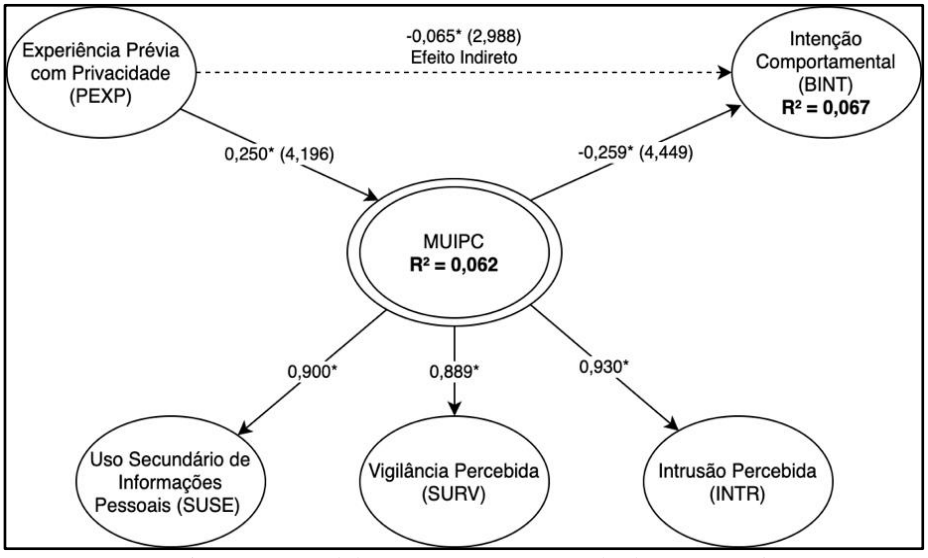

Figura 2 – Modelo MUIPC com os resultados (*p<0,05)
Fonte: Adaptado de Xu *et al.* (2012).

A tabela 7 (valores-p estimados por *bootstrapping* com 5000 repetições) detalha os coeficientes estruturais, valor-t, desvio padrão e valor-p e pode-se observar a relevância dos efeitos diretos da experiência prévia em MUIPC e de MUIPC com relação à intenção

comportamental e, assumindo um nível de significância de 5% ($p < 0,05$), é possível avaliar que todos os relacionamentos do modelo estrutural suportam todas as hipóteses propostas. Embora o efeito indireto de PEXP em BINT tenha apresentado significância estatística, o relacionamento foi fraco. Adicionalmente, o efeito direto da relação entre PEXP e BINT não atingiu o nível de significância assumido ($p < 0,05$), o que indica uma mediação total.

Tabela 7 – Resultados do Modelo Estrutural

Efeitos	Relação estrutural	Hipóteses e Avaliação	Coeficiente Estrutural	Desvio Padrão	Valor-t	Valor-p
Direto	PEXP → MUIPC	H1 - OK	0,250	0,059	4,196	0,000
Direto	MUIPC → BINT	H2 - OK	-0,259	0,058	4,449	0,000
Indireto	PEXP → MUIPC → BINT	H3 - OK	-0,065	0,022	2,988	0,003

Fonte: Elaborado pelos autores (2021).

5.4. Discussão dos resultados

Para atingir o objetivo desta pesquisa foi utilizado o modelo MUIPC e os resultados foram analisados através do instrumento PLS-SEM, que apontam que o modelo se mostrou capaz de confirmar as hipóteses propostas, ainda que com valores de R^2 baixos, sendo 6,2% de PEXP para MUIPC e de 6,7% de MUIPC para BINT.

A hipótese H1 foi confirmada para a amostra agrupada que apresentou influência positiva direta ($\beta=0,250$) com nível de significância $p < 0,001$ e um efeito pequeno ($f^2 = 0,066$) com R^2 em 6,2% na relação PEXP ® MUIPC e resultados similares aos encontrados em estudo anterior que mensura relação similar (Anderson e Agarwal, 2011), sendo que a relação se altera sensivelmente quando o segmento analisado é AGE2. Os valores ampliam para $\beta=0,336$, $f^2 = 0,13$ e $R^2 = 11,5\%$ e esses resultados confirmam a reflexão apresentada na literatura disponível que menciona que indivíduos de meia idade e idosos que experimentaram violação de privacidade no passado tendem a ter maiores preocupações com privacidade (Gupta e Chennamaneni, 2018).

Similar comportamento foi observado na confirmação da hipótese H2. Para a amostra agrupada MUIPC mostrou ter influência negativa direta ($\beta=-0,259$) com nível de significância $p < 0,001$ e um efeito pequeno ($f^2 = 0,072$) em BINT. A literatura corrente havia explicado o efeito negativo das preocupações com privacidade na intenção comportamental para divulgação de informações pessoais e de saúde dos indivíduos (Adjerid *et al.*, 2018) (Agarwal *et al.*, 2010) (Angst e Agarwal, 2009) (Yaraghi *et al.*, 2019) e este estudo veio confirmar que a mesma relação foi observada referente às preocupações com privacidade em m-Health.

Já com relação a H3, constatou-se que não há relação significativa direta entre PEXP e BINT e, embora, a relação indireta entre PEXP e BINT com MUIPC como construto mediador tenha sido comprovada, o coeficiente estrutural indicou uma relação fraca ($\beta=-0,065$) com nível de significância $p < 0,01$. Estudos anteriores corroboram este resultado ao explicar que experiência prévia com violação de privacidade afetam as crenças relacionadas aos riscos e confiança na adoção de determinada tecnologia (Malhotra *et al.*, 2004) e poder servir como um antecedente na relação entre as preocupações com privacidade e a intenção comportamental (Smith *et al.*, 1996). Como a intensidade dessa mediação é baixa, a descoberta contribui com a literatura ao abrir oportunidade para estudos futuros avaliarem a inserção de outros antecedentes no modelo, como o construto "Controle Percebido" (Heng, Hock-Hai, Tan e Agarwal, 2012) já que estudos anteriores mencionam que maior controle e proteção dos dados podem resultar em uma maior disposição dos indivíduos de revelar informações de saúde (Adjerid *et al.*, 2018).

Como abordado no decorrer deste estudo, m-Health, aplicativos móveis que armazenam e processam informações de saúde em *cloud computing* tem se apresentado como uma

tecnologia de interesse no segmento de saúde e examinar as preocupações com privacidade na ótica do indivíduo amplia a literatura disponível que foram em EHR e plataformas únicas de saúde.

7. Conclusões

Em linha com a literatura estudada, o objetivo desse estudo foi esclarecer o papel das preocupações com a privacidade na divulgação de informações de saúde e no uso de aplicativos móveis que as armazenam e processam na CC para buscar um melhor entendimento da relação entre os construtos preocupações com privacidade no uso de aplicativos móveis e intenção comportamental.

Como uma opção à EHR e prontuários únicos do paciente, os m-Health oferecem controle de acesso, consentimento sob decisão dos indivíduos e poder de processamento escalável enquanto implementam funcionalidades necessárias para prontuários únicos, seguindo padrões de mercado. Adicionalmente, como opção às funcionalidades de bem-estar, essas plataformas oferecem funcionalidades para troca de dados e acessibilidade. Dadas essas características, foi crítico entender as preocupações dos indivíduos quanto à privacidade na divulgação de dados nessas plataformas e antecedentes que afetam suas escolhas e observar o efeito nas pessoas de meia-idade e idosos. Esse estudo cumpriu, assim, seu objetivo e deu um importante passo ao avaliar m-Health como plataforma única de saúde e as implicações relacionadas com respeito às preocupações com privacidade, servindo como referência na avaliação das opções para mitigá-las.

Do ponto de vista prático, esse estudo deu foco no tópico crucial envolvido na adoção de uma plataforma de saúde: as preocupações relacionadas à privacidade. Ele aponta um caminho em direção ao uso de m-Health para unificação dos dados de saúde do indivíduo e sua digitalização, apresentando essa plataforma como uma opção às iniciativas em torno da criação de um prontuário único do paciente baseadas principalmente em EHR e o equilíbrio que estas plataformas oferecem em termos de segurança, privacidade e controle. Foi possível entender, dentro de um escopo definido, as preocupações com privacidade na ótica do indivíduo no uso de m-Health e foi possível avaliar a influência na disposição de se adotar essa tecnologia pelos indivíduos.

Esse estudo também traz contribuições teóricas relacionadas à privacidade de dados pois propõe o uso de uma escala adicional – MUIPC – em estudos na área de sistemas de informação para exame das preocupações com privacidade na área de saúde que, anteriormente, usavam principalmente escalas como CFIP ou CPM. Essa pesquisa reflete também o papel dos construtos vigilância e intrusão percebidas e uso secundário das informações no uso de m-Health pelos indivíduos. Assim, contribuições que emergem com este estudo mostram a relevância destas variáveis latentes e a preocupação com privacidade, fortalecendo a validade da escala MUIPC.

Futuros estudos podem investigar como provedores, fornecedores e seguradoras de saúde percebem as plataformas de m-Health em termos de funcionalidade, competitividade e controle de privacidade. Uma pesquisa mais aprofundada também pode esclarecer se o indivíduo é o principal influenciador em alavancar o uso destas plataformas ou se o papel em as disseminar está entre os outros envolvidos no segmento de saúde, como médicos, hospitais, clínicas, seguradoras ou outros prestadores. Há oportunidades para inclusão de construtos adicionais no exame das preocupações quanto à privacidade no uso de m-Health para correlacionar com a divulgação dos dados de saúde. Além disso, há espaço para estudar os benefícios percebidos no uso dessas plataformas, em adição às preocupações com privacidade.

Apesar de permitir generalizar os resultados considerando plataformas populares de m-Health, esse estudo não se limitou a uma plataforma específica e, dadas sutis diferenças entre

aplicativos atualmente disponíveis, há campo para se estudar e comparar os mesmos resultados em diferentes plataformas e segmentos demográficos.

Referências Bibliográficas

Adjerid, I., Adler-Milstein, J., & Angst, C. (2018). Reducing medicare spending through electronic health information exchange: The role of incentives and exchange maturity. *Information Systems Research, 29*(2), 341-361.

Agarwal, R., Guodong, G., DesRoches, C., & Jha, A. K. (2010). The digital transformation of healthcare: Current status and the road ahead. *Information Systems Research, 21*(4), 796-809.

Ahmad, O. B., Pinto, C. B., & Lopez, A. D. (2001). Age standardization of rates: A new who standard. *GPE Discussion Paper Series, 31*, 10-12.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469-490.

Angst, C. M., e Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly, 33*(2), 339-370.

Babbie, E. R. (1999). *Métodos de pesquisas de survey*. Belo Horizonte: Editora UFMG.

Chin, W., Marcolin, B., & Newsted, P. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a monte carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research, 14*, 189-217.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences (2nd ed.)*. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Creswell, J. W. (2012). Projeto de pesquisa: Métodos qualitativo, quantitativo e misto; tradução magda lopes – 3ª. edição. Porto Alegre: Artmed, 296 páginas, 2010. *Cadernos de Linguagem e Sociedade, 13*(1), 205-208.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management, 50*, 261-272.

Degirmenci, K., Guhr, N., & Breitner, M. (2013). Mobile applications and access to personal information: A discussion of users' privacy concerns. *In Proceedings of the International Conference on Information Systems (ICIS),* 2570-2590.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Gao, F., & Sunyaev, A. (2019). Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare. *International Journal of Information Management, 48*, 120-138.

Gilbert, M., & Cribbs, J. (2020). Hype cycle for consumer engagement with healthcare and wellness. **Gartner**, 12 aug 2019. Disponível em: https://www.gartner.com/en/documents/3989052/hype-cycle-for-consumer-engagement-with-healthcare-and-w. Acesso em: 15 jun 2021.

Gupta, B., & Chennamaneni, A. (2018). Understanding online privacy protection behavior of the older adults: An empirical investigation. *Journal of Information Technology Management, 29*(3), 1-13.

Hair, J., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017a). *A primer on partial least squares structural equation modeling - 2nd edition.* Newbury Park: Sage Publications, Inc.

Hair, J., Ringle, C., Sarstedt, M., & Gudergan, S. P. (2017b). *Advanced issues in partial least squares structural equation modeling.* Newbury Park: Sage Publications, Inc.

Heng, X., Hock-Hai, T., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342-1363.

Henseler, J., Ringle, C., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*, 115-135.

Hulland, J. (1999). Use of partial least squares (pls) in strategic management research: A review of four recent studies. *Strategic Management Journal, 20*(2), 195-204.

Juhee, K., & Eric Johnson, M. (2018). Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quarterly, 42*(4), 1043-1067.

Keil, M., Park, E. H., & Ramesh, B. (2018). Violations of health information privacy: The role of attributions and anticipated regret in shaping whistle-blowing intentions. *Information Systems Journal, 28*(5), 818-848.

Kim, S. H., & Kwon, J. (2019). How do ehrs and a meaningful use initiative affect breaches of patient information? *Information Systems Research, 30*(4), 1184-1202.

Kohli, R., & Tan, S. S.-L. (2016). Electronic health records: How can is researchers contribute to transforming healthcare? *MIS Quarterly, 40*(3), 553-574.

Lin, Y. K., Chen, H., Brown, R. A., Li, S. H., & Yang, H. J. (2017). Healthcare predictive analytics for risk profiling in chronic care: A bayesian multitask learning approach. *MIS Quarterly, 41*(2), 473-A473.

Liwei, C., Baird, A., & Rai, A. (2019). Mobile health (mhealth) channel preference: An integrated perspective of approach-avoidance beliefs and regulatory focus. *Journal of the Association for Information Systems, 20*(12), 1743-1773.

Malhotra, N. K. (2006). *Pesquisa de marketing: Uma orientação.* Porto Alegere: Bookman Editora.

Malhotra, N. K., Sung, S. K., & Agarwal, J. (2004). Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Mell, P. M., & Grance, T. (2011). *The nist definition of cloud computing*. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-145/final. Acesso em: 15 jun 2021.

Ozdemir, Z., Barron, J., & Bandyopadhyay, S. (2011). An analysis of the adoption of digital health records under switching costs. *Information Systems Research, 22*(3), 491-503.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Sambamurthy, V., & Zmud, R. W. (2017). *Guiding the digital transformation of organizations* - Second Edition. Legerity Digital Press.

Shapiro, C., Shapiro, C., & Varian, H. R. (1998). *Information rules: A strategic guide to the network economy*: Harvard Business School Press.

Silva Junior, S. D. *O efeito enquadramento nas decisões sobre a divulgação de informações pessoais: Um estudo experimental no âmbito dos aplicativos móveis.* 2015. 137 p. Tese (Doutorado em Administração) - Faculdade Administração, Contabilidade e Economia, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2015.

Silva Junior, S. D., Luciano, E. M., & Lübeck, R. M. (2020). Revalidação da escala mobile users' information privacy concerns para o contexto brasileiro. *Revista Eletrônica de Ciência Administrativa, 19*(2), 280-298.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477-564.

Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management, 34*(2), 177-184.

Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018). Privacy attitudes and data valuation among fitness tracker users. In*: Transforming Digital Worlds*. 229-239.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). *Measuring mobile users' concerns for information privacy.* In: International Conference on Information Systems, ICIS 2012.

Yaraghi, N., Gopal, R. D., & Ramesh, R. (2019). Doctors' orders or patients' preferences? Examining the role of physicians in patients' privacy decisions on health information exchange platforms. *Journal of the Association for Information Systems, 20*(7), 928-952.

Yaraghi, N., Ye Du, A., Sharman, R., Gopal, R. D., & Ramesh, R. (2015). Health information exchange as a multisided platform: Adoption, usage, and practice involvement in service co-production. *Information Systems Research, 26*(1), 1-18.