# mHealth: Privacidade e Fatores Humanos

**Wagner N. Silva**[1]

[1]Universidade Federal do Estado do Rio de Janeiro (UNIRIO)
CEP: 22290-240 – Rio de Janeiro – RJ – Brasil

wagner.silva@uniriotec.br

***Abstract.*** *Ensuring the privacy of information in mhealth environment is considered a challenge for its adherence and use, being addressed in many area research under information security, proposing methods and techniques that prevent unauthorized access to information. This research brings a different approach to privacy: one that concerns the desires and preferences of users technology in sharing their health information. Mobile mHealth, in addition to allowing data collection over extended periods of time and access to a broader range of information, directly or unrelated to patient health, enables the sharing of health information with various parties involved in the care, such as health professionals, caregivers, family members, etc. These factors make users' privacy desires and preferences dynamic by changing them based on different contexts. These dynamic contexts (focal point in this research) are not directly addressed in researches about this subject, making the issue of privacy one of the impact factors in the acceptance and use of this technology.*

***Resumo.*** *Garantir a privacidade das informações no ambiente mhealth é considerado um desafio para sua adesão e uso, sendo tratada em muitas pesquisas da área sob o viés da segurança da informação, com a proposição de métodos e técnicas que impedem o acesso não autorizado às informações. Esta pesquisa traz uma abordagem diferente de privacidade: a que diz respeito aos desejos e preferências dos usuários da tecnologia no compartilhamento de suas informações de saúde. Mobile mHealth, além de permitir a coleta de dados por longos períodos de tempo e acesso a uma gama mais ampla de informações relacionadas, diretamente ou não, com a saúde do paciente, essas tecnologias permitem compartilhar informações de saúde com diversas partes envolvidas no cuidado, como profissionais de saúde, cuidadores, familiares etc. Esses fatores fazem com que os desejos e preferências de privacidade dos usuários sejam dinâmicos, alterando-se baseados em diversos contextos. Esses contextos dinâmicos (ponto focal nesta pesquisa) não são diretamente tratados em pesquisas sobre o assunto, tornando a questão da privacidade um dos fatores de impacto na aceitação e uso da tecnologia.*

## 1. Contexto do trabalho

As inovações tecnológicas trouxeram muitos avanços para área da saúde, incluindo novas formas de cuidado. *mHealth* ou *mobile health* é a prática médica e de saúde pública apoiada por dispositivos móveis, como telefones celulares, dispositivos de monitoramento de pacientes, assistentes digitais pessoais (PDAs) e outros dispositivos sem fio [Global Observatory for eHealth 2016]. Trata-se de um subsegmento da *eHealth* (saúde

eletrônica), que aproxima a *eHealth* do paciente, a partir de dispositivos incorporados à sua vida diária, monitorando suas atividades e comportamentos e permitindo cuidados médicos personalizados.

De acordo com a Organização Mundial de Saúde (OMS) [WHO World Health Organization 2016]: "*Em muitos lugares, é mais provável que as pessoas tenham acesso a um telefone celular do que água limpa, uma conta bancária ou eletricidade*" . De fato, com o número cada vez maior de *smartphones* no mundo (cerca de 7 bilhões de dispositivo, mais de 70% em países de baixa ou média renda [ITU. United Nations agency for information and communication technologies 2015]), a tecnologia *mHealth* surge como uma oportunidade de ampliar o acesso aos serviços de saúde, prometendo inúmeros benefícios como: controle e monitoramento constante da saúde, precisão de diagnósticos e prevenção de novos problemas, redução de custos de serviços de saúde, viabilidade de atendimento a pessoas que vivem em áreas remotas, melhoria na comunicação médico-paciente, entre outros. Mesmo com tantos benefícios, a natureza sensível das informações que circulam nesses sistemas traz desafios de privacidade.

Privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar por si próprios quando, como e até que ponto as informações sobre eles devem ser comunicadas a outros [Westin 1967]. Trata-se de um conceito abstrato e subjetivo, ligado a percepção de cada indivíduo sobre o que representa uma ameaça à sua propriedade pessoal ou integridade física ou moral, dependendo de aspectos culturais (como religião, tradição, costumes, educação etc) e questões mais subjetivas como idade, estado de saúde, contexto atual [Rodrigues 2006].

No contexto *mHealth* a privacidade é ainda mais desafiadora, pois além de permitirem coleta de dados por longos períodos de tempo e acesso a uma gama mais ampla de informações relacionadas, diretamente ou não, com a saúde do paciente (por exemplo: localização, estilo de vida, interações sociais etc), essas tecnologias permitem compartilhar informações de saúde com diversas partes envolvidas no cuidado, como médicos e profissionais de saúde, cuidadores, familiares, operadoras de saúde etc [Avancha et al. 2012].

## 2. Problema Investigado

O surgimento da Internet e novas perspectivas de interação e comunicação entre indivíduos fizeram com que as pessoas passaram a enfrentar um número cada vez maior de decisões quanto à privacidade de suas informações. Decisões que perpassam desde aspectos de configuração de visibilidade em redes sociais até a opção por baixar um aplicativo para *smartphone* com base no acesso a dados confidenciais que ele solicita [Acquisti et al. 2017].

Os trabalhos sobre privacidade em *mHealth* na literatura preocupam-se com os aspectos técnicos da privacidade, relacionados a garantia da segurança das informações transmitidas via rede móvel e armazenadas no dispositivo ou em serviços de nuvem (*cloud*), para evitar o acesso não autorizado às informações do paciente [Silva et al. 2013] [Sharma et al. 2018]. Contudo, o uso colaborativo de tecnologia *mHealth* para gestão compartilhada de cuidados apresenta outras demandas de privacidade relacionadas a fatores humanos como, por exemplo, desejos e preferências do usuário no compartil-

hamento de suas informações de saúde com entes autorizados [Avancha et al. 2012].

Pesquisas relacionadas ao assunto não investigam especificamente os desejos e preferências de privacidade do usuário da tecnologia, considerando os contextos que fazem com que os usuários alteram suas preferências de privacidade. Contextos estes que possuem uma característica forte de ser dinâmico, variando constantemente na vida de um indivíduo decorrente de diversos fatores. Os dinâmicos contextos que alteram os desejos e preferências de privacidade dos indivíduos são os pontos focais desta pesquisa e não são diretamente tratados em pesquisas sobre o assunto, tornando a questão da privacidade um dos fatores de impacto na aceitação e uso da tecnologia.

## 3. Fundamentação e Trabalhos Relacionados

### 3.1. Fundamentação

Uma das teorias a qual esta pesquisa tem se apoiado é descrita pelo psicólogo social Irwin Altman, que em 1995 descreveu a teoria de regulação de privacidade. Essa teoria trata a questão da privacidade como "um seletivo controle de acesso ao indivíduo" através de um processo dialético e dinâmico de regulação de limites que são alterados de acordo com contextos. Na definição de privacidade de Altman o termo "dialético" se refere à disposição do indivíduo para se abrir ou fechar a outras pessoas, buscando ou evitando uma interação social. O conceito de "dinâmico", está no nível desejado de privacidade em um momento específico, podendo variar de acordo com contextos, ou seja, as pessoas modificam e reavaliam continuamente seus limites de acesso em resposta ao ambiente e às suas próprias necessidades de interação social.[Altman 1975, Villela 2016]

Outra teoria utilizada nesta pesquisa foi apresentada por Nissenbaum em 2004, ela é conhecida como a teoria de integridade contextual. Esta teoria considera que esses limites impostos pelos usuários são regidos por um conjunto de normas relacionadas à adequação social e ao fluxo de informação, que dependem do contexto. Com relação a adequação social, a norma determina que tipo de informação pessoal é apropriado compartilhar em determinada circunstância de acordo com o ambiente social a que o indivíduo está inserido, já o fluxo de informação, por sua vez, definem relacionamentos pela quantidade de informação que é compartilhada, as pessoas compartilham informações mais íntimas com amigos mais próximos e informação mais geral com os mais afastados. Nessa teoria, de acordo com Nissenbaum, as regras que mudam com o tempo, o que é compartilhado hoje, pode não ser mais apropriado amanhã.[Nissenbaum 2004, Villela 2016]

### 3.2. Trabalhos Relacionados

A preocupação com a privacidade em sistemas computacionais não é assunto recente. Em 1969, Hoffman [Hoffman 1969] já se preocupava com controle de acesso e privacidade dos sistemas existentes, percebendo o potencial dos mesmos de armazenar muitas informações pessoais sensíveis e os perigos do acesso ilícito de terceiros a essas informações. O autor, então, revisou as salvaguardas legais e administrativas para a proteção de informações sigilosas em computadores e as soluções técnicas que foram propostas à época. Em sua conclusão, Hoffman citou um autor contemporâneo a ele (Paul Baran) que menciona a responsabilidade dos engenheiros de computação de preservar o direito das pessoas à privacidade [Hoffman 1969].

Um trabalho recente e focado nos fatores humanos relacionados à privacidade é o de Barth e Jong (2017) [Barth and de Jong 2017] que realizaram uma revisão sistemática de literatura com o intuito de entender a paradoxo da privacidade *online*: usuários afirmam estar muito preocupados sobre sua privacidade, mas fazem muito pouco para proteger seus dados pessoais. A partir da leitura de 32 artigos completos, os autores identificaram 35 abordagens teóricas para tomada de decisão, concluindo que o paradoxo possui diferentes perspectivas, diferenciando a tomada de decisão de acordo com cálculos racionais e irracionais de risco-benefício e com o contexto no qual o paradoxo da privacidade ocorre [Barth and de Jong 2017].

No domínio de IoT (Internet das Coisas, do inglês *Internet of Things*), um cenário onde objetos habilitados para Internet interagem e cooperam entre si para atingir metas específicas, a invisibilidade da coleta, uso e compartilhamento de dados pode impactar a privacidade dos usuários dessas tecnologias. Duas revisões sistemáticas se destacaram neste domínio. O trabalho de Loukil *et al.* (2017) [Loukil et al. 2017] varreu a literatura em busca de soluções de preservação de privacidade em Sistemas de Informação Cooperativos, classificando os resultados obtidos em ciclo de vida dos dados, técnicas de preservação da privacidade e princípios de privacidade da ISO (*International Organization for Standardization*). Os autores concluíram que muitos problemas de proteção de dados e preservação da privacidade ainda precisam ser resolvidos em IoT e forneceram um conjunto de recomendações para consumidores e *designers* de aplicações IoT, a fim de informá-los sobre os pontos-chave para proteção dos dados e atendimento aos princípios de privacidade [Loukil et al. 2017].

Já a revisão sistemática de literatura empreendida por Aleisa e Renaud (2017) [Aleisa and Renaud 2017] apresentou uma visão geral das pesquisas relacionadas à privacidade em IoT, identificando que as pesquisas têm focado em análises das violações e ameaças de privacidade e no desenvolvimento de mecanismos de proteção da privacidade. Os autores destacaram a necessidade de mais pesquisas que envolvam os seres humanos no processo, considerando os poucos estudos observacionais e levantamentos (*surveys*) sobre violações e percepções da privacidade [Aleisa and Renaud 2017].

No contexto de mHealth, Avancha *et al.* (2012) [Avancha et al. 2012] propôs um *framework* de privacidade e empreendeu uma revisão de literatura com ênfase nas ameaças à privacidade, incluindo os desafios e oportunidades de criar interfaces humanas para permitir o gerenciamento de privacidade, além de buscar o entendimento sobre como os usuários percebem a privacidade, bem como sua importância para eles. Os autores finalizaram o artigo com um conjunto de questões de pesquisa em aberto sobre privacidade da tecnologia *mHealth* com foco no paciente [Avancha et al. 2012].

## 4. Objetivo da Pesquisa

Duas características já mencionadas nas seções anteriores referem-se ao fatores humannos e os contextos que fazem com que os usuários alterem suas preferências de privacidade a cada momento, porém esses contextos não são diretamente investigados sob o ponto de vista dos usuários nas pesquisas relacionadas ao assunto. Além disso, esses contextos possuem uma característica forte de ser dinâmico, variando constantemente na vida de um indivíduo decorrente de diversos fatores. Diante deste cenário, esta pesquisa busca investigar e identificar os contextos que fazem com que os usuários da tecnologia mHealth

alterem, dinamicamente, seus desejos e preferências de privacidade, tendo sempre como ponto de vista o usuário da tecnologia.

## 5. Métodos de Investigação

Para alcançar o objetivo proposto, primeiramente utilizou-se um procedimento de pesquisa bibliográfica, a partir do método de revisão sistemática de literatura. A escolha dos eixos comparativos foi feita com o intuito de responder a questão principal da revisão sistemática (identificação do estado da arte de pesquisas sobre privacidade em tecnologias *mHealth*, no que diz respeito a preferências e desejos do usuários).

Para tanto, buscou-se identificar as soluções propostas e métodos de pesquisa utilizados, bem como ilustrar os diferentes aspectos da privacidade em *mHealth* tratados pelos artigos, tais como tipos de ameaça à privacidade e a privacidade sob o ponto de vista dos usuários (suas demandas).

Além desses aspectos intrínsecos à privacidade, buscou-se também caracterizar o contexto das soluções *mHealth* apresentadas, a partir da identificação das abordagens de saúde tratadas, os domínios de aplicação considerados nas pesquisas e a presença (ou não) de abordagens colaborativas nas soluções.

Foi através desta revisão bibliográfica que ficou claro que as pesquisas relacionadas ao assunto não investigam especificamente os desejos e preferências de privacidade do usuário da tecnologia, considerando os contextos que fazem com que os usuários alteram suas preferências. Um outro achado foi a característica dinâmica dos desejos de privacidade do usuário devido devido principalmente a esses contextos.

Após essa revisão procura-se elaborar uma série de entrevistas com usuários em potencial desta tecnologia, onde primeiramente buscaremos identificar em qual perfil de privacidade ele se adequa. A paritir desta primeira análise, investigar as possiveis situações (contextos) fariam que eles alteraríam suas preferências de privacidade e porque isso acontece.

## 6. Planejamento dos Estudos

A pesquisa está sendo conduzida em 5 etapas. Na primeira etapa foi conduzida uma revisão sistemática da literatutra, a partir desta revisão foi identificado qual seria a contribuição da pesquisa. A etapa seguinte é a condução de uma série de entrevistas com potenciais usuários da tecnologia, o percurso metodológico das entrevistas ainda estão sendo definidos. Após as entrevistas será feito uma análise do discurso, buscando identificar os contextos que levam esses usuários a alterar suas preferências de privacidade nas tecnologias mHealth, como saída esta etapa produzirá um modelo baseado nesses contextos. Com base no achado da etapa anterior e para avaliar a pesquisa, será construido um aplicativo que considera como entrada as preferências do usuário e o modelo de contextos. Por fim, trabalharemos em um estudo de caso utilizando a ferramenta e analisando os dados coletados.

Atualmente estamos na finalização da primeira etapa da pesquisa, com os resultados aceitos em uma renomada conferência que ocorrerá em Janeiro 2020 no Hawaii (HICSS 2020), esta conferência tem como avaliação da Caepes Qualis A1.

## Agradecimento

Agradeço a professora Ana Cristina Bicharra Garcia pela orientação no tema.

## References

Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., and Schaub, F. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, 50(3):1–41.

Aleisa, N. and Renaud, K. (2017). Privacy of the Internet of Things: A Systematic Literature Review. *Hawaii International Conference on System Sciences 2017 (HICSS-50)*.

Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, and crowding.

Avancha, S., Baxi, A., and Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, 45(1):1–54.

Barth, S. and de Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7):1038–1058.

Global Observatory for eHealth (2016). Global diffusion of eHealth: Making universal health coverage achievable. Technical report, World Health Organization, Geneva, Switzerland.

Hoffman, L. J. (1969). Computers and Privacy : A Survey. I(2):19.

ITU. United Nations agency for information and communication technologies (2015). ITU releases 2015 ICT figures.

Loukil, F., Ghedira-Guegan, C., Benharkat, A. N., Boukadi, K., and Maamar, Z. (2017). Privacy-Aware in the IoT Applications: A Systematic Literature Review. In *On the Move to Meaningful Internet Systems. OTM 2017 Conferences*, pages 552–569, Rhodes, Greece. Springer, Cham.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, 79:119.

Rodrigues, V. J. d. S. (2006). *Gerência de Privacidade para Aplicações Sensíveis ao Contexto em Redes Móveis*. Phd thesis, Pontifical Catholic University of Rio de Janeiro.

Sharma, S., Chen, K., and Sheth, A. (2018). Towards Practical Privacy-Preserving Analytics for IoT and Cloud Based Healthcare Systems.

Silva, B. M., Rodrigues, J. J. P. C., Canelo, F., Lopes, I. C., and Zhou, L. (2013). A data encryption solution for mobile health apps in cooperation environments. *Journal of medical Internet research*, 15(4):e66.

Villela, M. L. B. (2016). Um modelo de design de privacidade para o compartilhamento de informações pessoais em redes sociais online.

Westin, A. (1967). *Privacy and Freedom*. New York, NY, USA.

WHO World Health Organization (2016). mHealth: use of mobile wireless technologies for public health. Technical report.