11-2019

Digital Health Privacy in Active-Aging Settings: Will the Law Let You Age Well?

Christopher Robertson

Tara Sklar

Richard Carmona

Kathie Insel

Arizona Legal Studies
Discussion Paper No. 20-04

Digital Health Privacy in Active-Aging Settings: Will the Law Let You Age Well?

Tara Sklar
Christopher Robertson
The University of Arizona
James E. Rogers College of Law

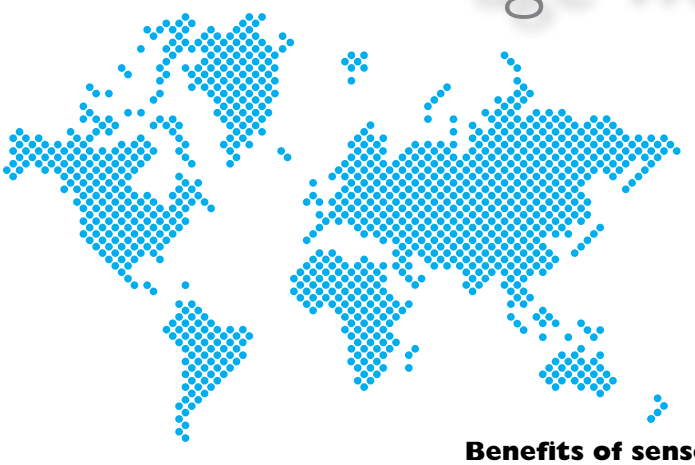
Richard H. Carmona
The University of Arizona
Zuckerman College of Public Health

Kathie Insel
The Universityof Arizona
College of Nursing

January 2020

Digital health privacy in active-aging settings:

Will the law let you age well?



Benefits of sensor surveillance and monitoring of personal data must be balanced with safeguarding protections, especially for cognitively impaired older adults

by Tara Sklar, JD, MPH; Richard Carmona, MD, MPH, FACS; Kathie Insel, PhD, RN; and Christopher Robertson, JD, PhD

What is privacy and how are our interpretations of it changing with advances in technology? This question, and concerns around potentially violating a person's right to privacy, have been emerging across industries around the world.

Senior living providers have increased their exposure to privacy risks with the shift to implementing sensors throughout their communities. Typically located in digital health devices that can be worn on the body or placed in the environment, these sensors are capable of collecting and tracking data relevant to a person's health and well-being on a continuous monitoring basis.

Continued on page 36

Digital health privacy in active-aging settings: Will the law let you age well?

Continued from page 34

There are privacy laws and a growing public awareness that this type of 24/7 surveillance—and the unprecedented detailed level of data it generates—should be accompanied by measures that support personal data protection. It is important to note that these privacy risks also apply outside the housing context. For example, seniors centers that use (or are planning to use) sensors to monitor participants and collect the generated data are similarly exposed.

The potential benefits in implementing digital health technologies are clear: to enable older adults to have a greater degree of independence and self-management, to decrease costs of care, and to improve quality and safety of care with real-time data. However, in the rush to adopt these technologies, many senior living communities and other service providers have yet to put in place essential safeguards and parameters around data collection, use and security.

Furthermore, overcoming age-related cognitive decline may be a barrier for some organizations to achieve informed consent for certain residents. Good intentions are not sufficient when there are significant legal, ethical and social implications to consider with continuous monitoring of a population where obtaining informed consent may prove difficult.

This article describes the current legal landscape around digital health privacy and proposes possible solutions for organizations to be forward-looking with the evolving laws and consent practices.

Benefits versus harms

The use of digital health technologies presents two sides of the same coin for senior living communities and other active-aging organizations. These benefits and harms are as follows:

Promises and discrimination risks. Digital health technologies are increasingly being credited with saving hundreds of thousands of lives[1] due to their ability to effectively monitor chronic diseases, namely cardiovascular disease. At the same time, they are responsible for creating unparalleled access to personal data. Unique, personal data are a high-priced commodity, which means there is a growing broker industry to aggregate and sell the data. This information often includes personal identifiers such as names, Social Security numbers, and addresses combined with health information such as running routes, heart rate history, dietary habits and sleep patterns.

Granular information can be used to help an individual receive timely, potentially life-saving care. Conversely, it could compromise individual privacy and result in discrimination against a person for life insurance, employment in later life or access to credit lines if perceived as a health risk. As technology comes into bedrooms—and bathrooms—some of our most intimate details may be exposed to watchful digital eyes.

Staffing. These technologies may allow a division of labor between humans and machines: Staff will have more time to interact with residents/members with high-touch human connectivity while the technology automates or accelerates the checking of vitals, medications and other daily routines. Nevertheless, there are concerns that these digital health technologies could lead to increased social isolation and loneliness for individuals, as their health status could be monitored from afar without regular check-ins by staff.

Family. Most families encourage the use of continuous monitoring for their loved ones for safety as well as to support independent living without constant caregiver oversight. However, using this technology might open the door to elder abuse if a family member wishes to demonstrate incompetence or a disability in order to gain greater control over a relative's finances and medical decisions.

Increased health anxiety. Currently, there is little research on how anxiety over one's health changes over the life span. Generally, as people age they are more likely to experience a serious illness or chronic disease, which creates greater risk for health anxiety.[2] This anxiety can contribute to increased utilization of healthcare services with doctor visits, lab tests and medications.

It is not clear if residents' access to real-time data via digital health technologies would relieve or exacerbate the higher risk for health anxiety. Either way, it would have implications for healthcare utilization later in life and be a fruitful area for further exploration.

Legal landscape around digital health privacy

Digital health privacy sits in a developing legal landscape where technology advances much faster than the law, which leaves senior living organizations and other service providers in a lurch as to how to act.

In brief, the concept of privacy is consistently described and recognized as the right of an individual to limit the collection, use and dissemination of personal information. A patchwork of laws and regulations exist in the United States and abroad, but the unifying theme is that individuals have a right to protect information about themselves and ensure it remains private. In addition, organizations have legal and ethical requirements to implement safeguards that will protect the private information they collect.

At its heart, privacy is about ensuring that the expectations of individuals are met and their data are not misused.

A growing number of privacy laws are sometimes perceived as barriers to

implementing these new digital health technologies. Among these laws are:

- Health Information Portability and Accountability Act (HIPAA) in the United States
- General Data Protection Regulation (GDPR) in Europe
- Protecting Personal Health Data Act (PPHDA), a proposed federal data privacy law for Americans

Additional sector-specific laws to protect personal data from misuse include the Americans with Disabilities Act, Fair Credit Reporting Act and federal and state laws to protect against consumer discrimination.

This article describes what HIPAA covers and where there are gaps specific to digital health privacy that the GDPR and PPHDA could shore up.

HIPAA. Enacted in 1996, this federal law establishes standards for the privacy and security of protected health information (i.e., identifiable information used in connection with healthcare treatment, payment or operations). A prominent component of HIPAA is the "Privacy Rule."[3] The goal of this rule is to protect patients' health information, while allowing a flow to covered entities, which consist of healthcare providers and plans or related business associates. Senior living communities and centers that provide healthcare and bill Medicare or other health plans are considered covered entities. Business associates could include any company helping the healthcare provider or plan provide a number of services like managing claims, quality assurance and legal or financial services.

The definition of a covered entity is important because these entities are required to obtain written authorization from patients regarding use or disclosure of their health information that is not for treatment, payment or general healthcare operation.

University of Arizona presenters explored potential privacy risks and solutions related to digital health technologies with senior living leaders at the ICAA Fall Forum 2019. Image courtesy of Tara Sklar

The rub is that *digital health manufacturers are not covered entities under HIPAA*. They therefore are not subject to the compliance requirements, including written authorization/consent. The only time HIPAA would protect personal data collected by a digital health device is if that manufacturer/distributor has a contract with a healthcare provider or plan (a covered entity) to provide patient services. Even if HIPAA could apply under that contacting scenario, it would still be downstream, meaning post-collection of data where harm or violation of privacy to an individual has already occurred.

GDPR and PPHDA. In contrast, the GDPR from the European Union (EU) takes a more upstream approach than HIPAA and has four key principles[4]:

- Personal data can be collected only for a specific purpose.
- The person must be informed of and consent to the purpose for the data collection.
- Only as much data as is necessary to achieve that purpose should be collected.
- The collected data must be deleted at the request of the participant, or when it is no longer needed for the purpose for which it was collected.

The GDPR went into effect in May 2018 and applies to any organization that processes data in the EU. It provides individuals greater control over their personal data with the ability to access, amend or delete their data. The GDPR also increases accountability among companies by requiring them to prove compliance, such as proof of obtaining affirmative consent, and has hefty fines for noncompliance.

The principles of GDPR are notable in light of a proposed bipartisan US federal bill, PPHDA,[5] which was introduced in the Senate in June 2019. This bill is drafted with the intent to shore up HIPAA

Continued on page 38

Digital health privacy in active-aging settings: Will the law let you age well?

Continued from page 37

A word cloud illuminates discussion of digital health privacy risks and solutions at the ICAA Fall Forum 2019, held in conjunction with ICAA's conference in October. Image courtesy of Tara Sklar

and align it with the GDPR. International companies are finding they have to comply with GDPR and some, including Microsoft CEO Satya Nadella,[6] have made a global call to advocate a "GDPR for the World" and prevent further privacy laws from surfacing that could increase compliance costs.

The PPHDA would operate similarly to the GDPR, where disclosures to obtain consent must be written in clear, concise, easily accessible language and at an appropriate reading level. Should this federal effort fail, as is the likely scenario with most proposed legislation, then state action may be another route. California has a pending digital health bill (AB 2167) that contains many features from the PPHDA. It is significant that both the GDPR and PPHDA define and require informed consent. Specifically, individuals will receive information about what they are agreeing to, the risks and benefits along with the alternatives, and that it is a voluntary decision, which they (or their surrogate) are competent to make at the time.

Unfortunately, a common practice with consent is to treat it as a one-off with a lot of fine print at a high reading level. Also, comprehension is not generally tested to see if the signee understands terms. Undertaking measures to obtain informed consent can be challenging with any population, and these challenges are elevated when working with an older population where age-related cognitive decline is more prevalent.

Possible solutions

There are possible solutions to mitigate the potential privacy risks associated with continuous monitoring in senior living and other settings and to improve practices around informed consent.

To further explore these risks and solutions, we formed a multidisciplinary research team from the University of Arizona's Colleges of Law, Nursing and Public Health and collaborated with the International Council on Active Aging's 2019 Annual Fall Forum, in October. The ICAA Forum brought together approximately 80 industry leaders from senior living providers across the US. As researchers, we presented to participants the benefits as well as legal, ethical and social implications in adopting these new technologies.

Together with industry leaders, we proposed the following strategies to transform these challenges:

Data generation and access. There should be a greater recognition in the field that not all data are good data and to make efforts to reduce enormous quantities of sensitive data being gathered without an overall purpose for how to use this information.

The potential uses around this type of data, including promoting overall wellness, can make this determination difficult. It may help to consider the data in light of tests and procedures regularly offered in the medical care system where, for example, just because we could order an MRI [magnetic resonance imaging] screening does not mean we always should. Many of these technologies are capable of tracking a wide variety of health metrics like basic vitals such as weight, sleep, heart rate, etc. But they can also collect and track data on a much broader range of variables from muscle function, ketones in the blood [substances signaling low insulin levels], mood, and vitamin deficiencies.

Similar to results from an MRI, the generated data may be interesting. Without a clear plan for how to use collected data, however, it may prove to be a suboptimal use of resources for a provider and place an unnecessary burden on a person's privacy.

One strategy is to adopt the GDPR principles of "data can only be collected for a specific purpose" and "collect only as much as is minimally necessary to achieve that purpose" in internal policies and procedures. These steps could both promote protections for individual privacy as well as prevent against inefficiencies with analysis paralysis due to too much data.

Continued on page 40

Digital health privacy in active-aging settings: Will the law let you age well?

Continued from page 38

Resources

Internet

ADA.gov (US Department of Justice, Civil Rights Division): Information and Technical Assistance on the Americans with Disabilities Act
www.ada.gov

Federal Trade Commission: Fair Credit Reporting Act
www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act

HealthIT.gov (Office of the National Coordinator for Health Information Technology): Security Risk Assessment Tool
www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Stay Safe Online (National Cyber Security Awareness Alliance)
https://staysafeonline.org

UK Government Information Commissioner's Office
https://ico.org.uk/

*** Data protection self assessment**
https://ico.org.uk/for-organisations/data-protection-self-assessment/

*** Guide to Data Protection**
https://ico.org.uk/for-organisations/guide-to-data-protection/

*** Guide to the General Data Protection Regulation (GDPR)**
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

US Department of Health and Human Services, Office for Civil Rights: The HIPAA Privacy Rule
www.hhs.gov/hipaa/for-professionals/privacy/index.html

University of Arizona College of Nursing
https://nursing.arizona.edu

University of Arizona James E. Rogers College of Law
https://law.arizona.edu

University of Arizona Mel and Enid Zuckerman College of Public Health
https://publichealth.arizona.edu

Print

McGraw, D., & Kuraitis, V. (2019, August 19). Protecting Health Data Outside of HIPAA: Will the Protecting Personal Health Data Act Tame the Wild West 2. *The Health Care Blog*. Available at https://thehealthcareblog.com/blog/2019/08/19/protecting-health-data-outside-of-hipaa-will-the-protecting-personal-health-data-act-tame-the-wild-west/

Miller, M. (2019, June 14). Klobuchar, Murkowski introduce legislation to protect consumer health data. *The Hill*. Available at https://thehill.com/policy/technology/448606-klobuchar-murkowski-introduce-legislation-to-protect-consumer-health-data

US Department of Health and Human Services. (2016). Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA. Available at www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf

US Department of Health and Human Services, and Healthcare & Public Health Sector Coordinating Councils. (2018). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Available at www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Several questions could help with this process of limiting data collection, including:

- What is the data for?
- Why is it important?
- How long will it be needed
- Could it be reused for a related purpose?

There is also an opportunity for senior living organizations and other providers to partner with universities and researchers to optimally use and interpret data. This type of collaboration could help narrow responses to the aforementioned questions and identify patterns for predictive analytics with specified data to achieve organizational goals, such as better quality and safety.

Quality oversight. Policies and procedures are also recommended to address any increased liability exposure and legal risks for organizations that collect 24/7 real-time data. An example is standards for the frequency in which data will be reviewed and responded to if there are signs of abuse, neglect or poor quality care. Additionally, policies around technology failure, ranging from data security breaches to interoperability barriers with other systems, should be clearly defined before technology is implemented.

Ongoing engagement and education. A hopeful vision is a future in which staff will be able to increase the level of personalized care and interact with residents/members one-to-one to build stronger human connections with less focus on recording daily activities or vitals. However, simply investing and setting up these digital health technologies will not necessarily lead to more staff and resident interactions.

Ongoing programmatic support will be necessary to support such a change in focus with availability for staff, residents, caregivers and family members.

As the technology will continue to evolve, so should the training for all those involved.

Consent practices. Similar to adopting GDPR principles to limit data generation and access, the following questions offer guidance in drafting consent forms:

- What data should be collected by the resident/member for a specific purpose and how long will it be stored?
- What information would a "reasonable person" need in order to decide whether to participate? Consider factors that could influence the desire of a resident/member to participate or to opt out.
- Who will have access to the data? How will it be shared and secured?

In the consent forms, it would help to highlight key terms that would be material in terms of influencing a person's decision to participate. The GDPR and PPHDA both emphasize the importance of plain language provided at an appropriate reading level. In communicating the consent forms, organizations may want to use multimedia decision aids, narratives and well-trained counselors to test comprehension and ensure terms are understood. It is also possible to allow for a more dynamic consent process that takes place periodically as opposed to a one-off. Emphasizing the voluntary nature of the consent process with an opt-out provision is encouraged, to help ensure a level of autonomy for individuals to decide their preferred amount of privacy with technologies.

Broadening safeguards, meeting expectations

Protecting privacy rights while using digital health technology to monitor care and potentially save lives is a key legal issue today in digital health systems. In trying to keep up with the best in assistive technologies, senior living organizations and other providers can find challenges in planning for and implementing safeguards around data collection, use and security.

All organizations would benefit from adopting a cautious approach to implementing digital health technologies that incorporates principles from the GDPR and practices that help ensure informed consent. The GDPR is not the law of the land in the United States, but its principles are being adopted by an increasing number of international companies, given that the movement of data does not necessarily follow country jurisdictional lines. Drafting and implementing internal policies and procedures *now* that align with the GDPR will help organizations become forward-looking with future digital health privacy laws that will inevitably surface in their states or federally.

In the meantime, this strategy provides a framework for intentional data use that attempts to not unduly infringe on the privacy rights of individuals, yet also

Continued on page 42

2019 Snapshot: Senior living communities report using these types of digital health technologies

Wearables
Fitbit, Garmin, Apple Watch often paired with fitness equipment, scales, and apps on smartphones VirtuSense Wander Guards Sneakers with GPS [Global Positioning System] Pendants and Handheld mobile technology to support alerts/life alert
Environment
Alexa Smart Toilet (track deficiencies, dehydration, urinary tract infections) Smart homes Cameras (detect falls) Pressure and motion sensors (Billy) Chair sensors and alarms Bed sensors / smart beds
Workforce
Cameras, sensors and software to monitor locations of employees: Verify tasks, reduce workforce issues and encourage interactions with residents
Robotics and interactive digital health programs
ElliQ Robot: To support social interactions, environment scans Jintronix: Rehab program with analysis and treatment recommendations Sagely: Tracks resident engagement and wellness metrics

Figure 1. 2019 Snapshot: Senior living communities report using these types of digital health technologies.

Digital health privacy in active-aging settings: Will the law let you age well?

Continued from page 41

helps organizations clearly define their data protection practices in a quickly expanding digital era.

Tara Sklar, JD, MPH, is professor of health law and director of the Health Law & Policy Program at the University of Arizona, located in Tucson. At the University of Arizona, Sklar oversees multidisciplinary, online programs in health law, including new Graduate Certificates in Aging Law & Policy and Health Information Privacy & Data Security that are part of the Master of Legal Studies. She teaches and writes primarily in how laws and policies influence the health and well-being of older adults. Her research has been published in the New England Journal of Medicine, Journal of Empirical Legal Studies, Annals of Health Law & Life Sciences, *and* The Elder Law Journal, *among others. Prior to her current role, Sklar was the inaugural director of aging programs and established the first multidisciplinary, online Master of Aging degree across eight colleges at the University of Melbourne in Australia.*

Richard H. Carmona, MD, MPH, FACS, had a distinguished career in public health, serving as 17th Surgeon General of the United States. His interest in public health stemmed from the realization that most of his patients' illnesses and injuries were preventable. Today, Carmona serves as chief of health innovations for Canyon Ranch, a global leader in the wellness movement. He is a distinguished professor, Zuckerman College of Public Health, University of Arizona.

Kathie Insel, PhD, RN, is a professor and interim chair of the biobehavioral division in the College of Nursing at the University of Arizona. Her work focuses on improving self-management of chronic conditions among older adults, with the goal of maintaining independence for as long as possible. Insel was able to demonstrate a 35% improvement in older adults consistently taking antihypertensive medications among those who used prospective memory strategies compared to an education and attention control condition.

Christopher Robertson, JD, PhD, is associate dean for research and innovation at the University of Arizona, where he founded the Regulatory Science Program. He is also a principal with Hugo Analytics, which provides scientific case evaluation and optimization services. In addition to dozens of articles, Robertson has coedited two books, Nudging Health: Behavioral Economics and Health Law *(2016) and* Blinding as a Solution to Bias: Strengthening Biomedical Science, Forensic Science, and Law *(2016). In 2019, Harvard University Press is publishing his new book,* Exposed: Why Health Insurance is Incomplete and What Can be Done About It.

References

1. Dolan, B. (2014, December 16). Prediction: Health wearables to save 1.3 million lives by 2020. *MobiHealthNews*. https://www.mobihealthnews.com/39062/prediction-health-wearables-to-save-1-3-million-lives-by-2020
2. Burling, S. (2019, October 2). Health anxiety tends to rise after age 50. It doesn't have to take over your life. *Medical Xpress*. https://medicalxpress.com/news/2019-10-health-anxiety-age-doesnt-life.html
3. US Department of Health and Human Services. (2015, April 16). The HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
4. UK Government Information Commissioner's Office. (2019, 25 April). Guide to the General Data Protection Regulation (GDPR). https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
5. Miller, M. (2019, June 14). Klobuchar, Murkowski introduce legislation to protect consumer health data. *The Hill*. https://thehill.com/policy/technology/448606-klobuchar-murkowski-introduce-legislation-to-protect-consumer-health-data
6. Hamilton, I. A. (2019, January 24). Microsoft CEO Satya Nadella made a global call for countries to come together to create new GDPR-style data privacy laws. *Business Insider*. https://www.businessinsider.com/satya-nadella-on-gdpr-2019-1