

Viewpoint

Mind Your Data: Privacy and Legal Matters in eHealth

Catharina M L Zegers^{1,2,3}, PhD; Annemieke Witteveen^{1,4}, PhD; Mieke H J Schulte^{1,5}, PhD; Julia F Henrich^{1,6}, PhD; Anouk Vermeij^{1,7}, PhD; Brigit Klever^{1,8}, PhD; Andre Dekker^{1,3}, Prof Dr

¹Digital Society Health & Well-being, The Hague, Netherlands

²Institute of Data Science, Maastricht University, Maastricht, Netherlands

³Department of Radiation Oncology (MAASTRO), GROW - School for Oncology and Development Biology, Maastricht University Medical Centre, Maastricht, Netherlands

⁴Department of Biomedical Signals and Systems, TechMed Centre, University of Twente, Enschede, Netherlands

⁵Department of Clinical, Neuro and Developmental Psychology, Vrije Universiteit, Amsterdam, Netherlands

⁶Unit of Health, Medical and Neuropsychology, Institute of Psychology, Leiden University, Leiden, Netherlands

⁷Department of Cognitive Neuropsychology, Tilburg University, Tilburg, Netherlands

⁸University Medical Center, University of Groningen, Groningen, Netherlands

Corresponding Author:

Catharina M L Zegers, PhD

Institute of Data Science

Maastricht University

Paul-Henri Spaaklaan 1

Maastricht, 6229 ER

Netherlands

Phone: 31 43 388 4996

Email: karen.zegers@maastrichtuniversity.nl

Abstract

The health care sector can benefit considerably from developments in digital technology. Consequently, eHealth applications are rapidly increasing in number and sophistication. For successful development and implementation of eHealth, it is paramount to guarantee the privacy and safety of patients and their collected data. At the same time, anonymized data that are collected through eHealth could be used in the development of innovative and personalized diagnostic, prognostic, and treatment tools. To address the needs of researchers, health care providers, and eHealth developers for more information and practical tools to handle privacy and legal matters in eHealth, the Dutch national Digital Society Research Programme organized the “Mind Your Data: Privacy and Legal Matters in eHealth” conference. In this paper, we share the key take home messages from the conference based on the following five tradeoffs: (1) privacy versus independence, (2) informed consent versus convenience, (3) clinical research versus clinical routine data, (4) responsibility and standardization, and (5) privacy versus solidarity.

(*JMIR Form Res* 2021;5(3):e17456) doi: [10.2196/17456](https://doi.org/10.2196/17456)

KEYWORDS

data; privacy; eHealth

The Digital Society Program

The Association of Universities in the Netherlands (VSNU) has brought together scientists from all 14 universities in the Netherlands to address the pressing questions raised by the emergence of a digital society. Exploring the responsible use of innovative digital technologies in the health care sector has high societal priority because of the potential to significantly improve health care and reduce health care costs. The Health & Well-Being program line of the VNSU Digital Society Research Programme aims to develop, evaluate, and implement

integrated and personalized digital health care solutions, while addressing the societal challenges raised by the digitalization of health care.

Decelerating factors in the development and implementation of eHealth are a lack of knowledge, information, and practical tools with respect to handling privacy and legal matters. To discuss these factors, the Digital Society Health & Well-Being team organized a conference on September 26, 2019 titled “Mind Your Data: Privacy and Legal Matters in eHealth” with the aim to learn from each other’s approaches to tackle privacy and legal matters in the development of eHealth.

The conference hosted five speakers who were selected based on their unique backgrounds (law, eHealth, data science, philosophy, and mobile health [mHealth]), vision, and expertise on privacy and legal issues in eHealth. Marie-José Bonthuis is an external privacy lawyer who is connected to the Medical Biobank Lifelines and to the University Medical Center Groningen. Furthermore, she is an expert in the Health Research Infrastructure initiative (Health-RI) service desk for ethical, legal, and societal questions related to personalized medicine and next-generation sequencing. Dr. Bonthuis presented a talk titled “Overview of data protection principles in research: bringing practice and legislation together.” Niels Chavannes is a professor of Public Health and Primary Care at Leiden University Medical Centre, a general practitioner, and the founder of the National eHealth living lab (NeLL). Professor Chavannes presented a talk titled “Clinical implementation of successful eHealth initiatives: ethical and legal issues.” Andre Dekker is the professor of Clinical Data Science at Maastricht University, Maastricht University Medical Center+, and MAASTRO Clinic. Professor Dekker presented a talk titled “The personal health train: privacy preserving learning from health data.” Peter Paul Verbeek is the professor of Philosophy of Technology and scientific codirector of DesignLab of the University of Twente. In addition, he is an honorary professor of Techno-Anthropology at Aalborg University and chair of the UNESCO World Commission for the Ethics of Science and Technology. Professor Verbeek shared his perspective in a talk titled “Privacy and beyond: inclusive digitalisation and the dynamics of privacy.” Finally, Edward Watkins is the professor of Experimental and Applied Clinical Psychology at the University of Exeter. Professor Watkins presented a talk titled “ECoWeB – mental health app for young people data and governance issues.”

More than 100 participants from a wide range of organizations (universities, medical centers, knowledge institutes, private parties, citizens, and government) attended the conference. Three independent authors noted down specific points that were expressed during the presentations, panel discussion, and eHealth forum. These notes were compared, sorted in categories, and juxtaposed in a way that the ethical challenges clearly emerged. Solutions provided by speakers were described; otherwise, clarification was provided by the authors of the paper. This resulted in our summary of the most prominent ethical-, technical-, and research-related issues in eHealth and their potential solutions.

Privacy Versus Independence

There is no straightforward answer for the best way to address privacy issues in eHealth. For each eHealth application, there should be a balance between individual privacy and potential individual or societal benefit. Data protection is all about contextual integrity; that is, using data responsibly within a specific context. Take for example the development of an mHealth approach to assess and enhance emotional competence for well-being in the young (ECoWeB project) [1]. In this project, young people expressed their reluctance to share passive sensor data and preferred to be in control of the data they would like to release. In this situation, an active approach to gather

data (eg, by questionnaires) is most suitable. By contrast, the use of cameras, a more privacy-intrusive method, is more likely to be accepted in smart homes for people with dementia, since the benefit for the user is larger, as people could have the opportunity to stay at home for a longer time [2]. This is in agreement with Wilkowska et al [3], who showed that female patients and healthy adults insist on higher security and privacy standards, whereas people with ailing health consider privacy of lower importance. End users seem to be willing to tradeoff part of their privacy for the benefit of, for example, independence.

To gain insight into this tradeoff, user preferences, and needs, it is essential to include the end user in the design of eHealth at an early stage of development. This should provide an understanding as to what extent the user is willing to share data and for what purpose. During the conference, this was exemplified by the ECoWeB project [1] in which co-design with young people was critical. The data collection and recruitment are fully online processes, and the use of data is transparent and clear to the users. Previous research has shown that the uptake of eHealth and mHealth is only successful when they are built to fulfill a certain need of either patients or health care providers [4]. The early involvement of clinicians and patients will encourage adoption and maximize the positive impact of an intervention [5]. An example of a dedicated approach to develop and evaluate eHealth is the Centre for eHealth and Wellbeing Research roadmap developed by van Gemert et al [6], which focuses on user participation and process evaluation.

Informed Consent Versus Convenience

eHealth research generally includes an informed consent procedure for use and accessibility of data. This can potentially be done by digital authentication, including, for example, parental consent and age verification. However, during the conference’s panel discussion, the issue about how elaborate digital informed consent should be arose. The panelists concluded that there should be a balance between simple, convenient, and easy to understand versus fully complete. This tradeoff is similar to a paper-based consent procedure. Nevertheless, there seems to be a striking difference between the requirements for informed consent of eHealth in comparison to commercial applications. An editorial published in *Nature* [7] also addressed this issue, stating that the consent for commercial mobile applications is often not more than a box to tick, with terms and conditions that are hardly ever read by the users.

In addition to informed consent, it is highly important to address the expectations of the eHealth app. This includes information on the procedure for incidental findings, such as whether or not the user wants to be actively informed or what can be expected with regard to automated messaging/triggering the health care provider for actions in the case of a monitoring app. Providing this additional information might limit possible overexpectations of users of the app.

Clinical Research Versus Clinical Routine Data

Data obtained after informed consent are only available from a small population of people that are registered for clinical research or use a specific eHealth app. By contrast, general registries collect data from a large number of patients, but the information is limited to demographics and a small selection of clinical variables. Another data source is clinical routine data, which contains the largest amount of clinically relevant information. One could think of a “patients like me” approach, where we can learn from existing data worldwide to find a similar patient. Unfortunately, clinical routine data are very hard to collect centrally because they are stored in individual local databases. One of the potential solutions is the use of distributed learning. The Personal Health Train is an example of this, where the data remain at the source (eg, the hospital) in Findable, Accessible, Interoperable, Reusable (FAIR) data stations, and the analysis method (eg, the algorithm) is transferred to the data. This method has been successfully implemented such as for predicting the 2-year survival of lung cancer patients using clinical data of 20,000 patients [8,9].

To allow for the secondary use of clinical personal data, data should be made nonidentifiable or anonymous [10], however, it is unclear when data are truly anonymous. Complete anonymity cannot be guaranteed if combinations of demographic data are given, and thus the question as to when data are truly anonymous remains. Many datasets that appeared to be anonymous have been released and individuals were reidentified [11]. Reidentification is generally performed by media or researchers, with the aim to show that shared data are unsafe, to publish new algorithms, and show weaknesses in the databases. An example was the reidentification of an individual from an adverse events database of Health Canada, and the media were able to reidentify a deceased woman based on a match of age, location, and date of death [12]. Algorithms such as k-anonymity can be used to describe the level of anonymity of datasets that plays a role in the definition of (non)identifiable personal data [13]. In addition, to determine the likelihood of an individual to be correctly reidentified, Rocher et al [11] proposed and validated a statistical model that was able to reidentify individuals even if the dataset was heavily incomplete. As such, if a dataset has been completely anonymized, it would be impossible to find the data of an individual who would like to withdraw consent to use their data. This is problematic if participants have been informed that they can withdraw their consent at any time [7]. An additional problem occurs in research scenarios that require data to be linked across different entities (eg, linking medical data from a hospital to socioeconomic data from Statistics Netherlands). These scenarios demand separate solutions that address privacy while still enabling subject-level linking based on common information [14].

Responsibility and Standardization

There are no straightforward answers to the questions of who is responsible for digital health apps, and how to guarantee

maximal privacy and compliance with legislation. Together with multiple partners, the VSNU developed a Code of Conduct for research integrity in the Netherlands in 2018. The responsibilities have been defined at multiple levels, from the individual researcher to the boards of research institutions and the institutions as a whole [15]. Researchers can also use the General Data Protection Regulation (GDPR) carwash [16], a prototype of a practical flowchart that aims to guide researchers through the necessary steps to work with personal data in a GDPR-compliant manner.

Moreover, it is hard for a user to determine which app is qualitatively good. The availability of health apps is increasing rapidly. Pereira-Azevedo and Venderbos [4] estimated that over 300,000 medical apps were available in 2018. Medical App Checker developed by the Royal Dutch Medical Association was established as an initiative to evaluate mobile medical apps [17]. Medical App Checker consists of several checklists, including one for evaluating the protection and security of personal data. Additionally, an international norm (ISO standard) is in development for health and wellness apps. This standard could be used to certify apps that meet the norms for safety, reliability, and user-friendliness based on existing quality requirements and legislation. The latter is in flux as the new EU Medical Device Regulation, which takes effect on May 2021, will set more stringent demands on medical applications.

Finally, when moving from research toward the clinical implementation of eHealth, Dutch professional communities (medical specialists, medical physics, and clinical informatics) have expressed in their vision statements that they will take their responsibilities in the stimulation of the development and use of eHealth, and to assure its quality and safety.

Privacy and Solidarity

Technological innovations change our society rapidly and the interaction of humans with these digital innovations may also influence our perception of societal values such as privacy. The complex interactions of how innovations influence the ethical frameworks with which they are valued can be exemplified with a Google Glass study. In this study, a technological mediation approach was used to focus on the dynamics of the interaction between technologies and human values. Online discussions about Google Glass technology were investigated to evaluate how people articulate new meanings of the value of privacy [18].

Additionally, there are cultural differences in the way we value privacy, especially on a global scale. To account for this dynamism of values, value-sensitive and responsible design approaches should be adopted. There is also a movement toward solidarity and data donorship. Toward this end, a culturally sensitive balance should be sought between sharing (“give data and save lives”) and protection (eg, potential threat of commercial exploitation) of data.

Conclusion

The information presented and discussed at the conference highlighted the many tradeoffs in eHealth with regard to privacy

and legal questions. To prevent potential decelerating factors in the development and implementation of eHealth, we need to be aware of these tradeoffs between (i) privacy and independence, (ii) informed consent and convenience, (iii) clinical research and clinical routine data, (iv) responsibility and standardization, and (v) privacy and solidarity. Furthermore, we need to make use of the available knowledge and tools on

a national and international level, think carefully about the design of the application, and include end users at an early stage of development to reach the full potential of the eHealth technology. Clearly, there are risks associated with developments in eHealth, but rather than avoiding risks and stalling innovation, we should attempt to minimize risks while providing the greatest possible benefits to society.

Acknowledgments

We would like to thank the VSNU, the Digital Society program coordinators (Prof I Lagendijk, Prof M de Rijke, and Prof S Wyatt), our colleagues of the Health & Well-Being team and co-organizers of the conference (Prof A Brombacher, Prof A Evers, Prof E Feskens, Prof H Hermens, Prof L van Gemert-Pijnen, Prof N Maurits, Prof H Riper, Prof M Sitskoorn, Dr I Kalinauskaite, Dr J van Soest, Dr R Fijten, Dr R van der Vaart, Dr S van Dijk, Dr M Simons, Dr M Tabak, and Dr K Gehring), the speakers, including external privacy lawyer Marie-José Bonthuis, Professor of Public Health and Primary Care at Leiden University Medical Centre; general practitioner and the founder of the National eHealth living lab (NeLL) Niels Chavannes; Professor of Clinical Data Science in Maastricht Andre Dekker; Professor of Philosophy of Technology at the University of Twente and chairman of UNESCO's World Commission on the Ethics of Scientific Knowledge and Technology Peter Paul Verbeek; and Professor of Experimental and Applied Clinical Psychology at the University of Exeter Edward Watkins. We also thank all (forum) participants at the event.

Conflicts of Interest

None declared.

References

1. ECoWeB Project. URL: <http://www.ecowebproject.eu/> [accessed 2019-10-17]
2. Wrede C, Jansen L, Havinga PJM, Croockewit JH, van Gemert-Pijnen JEW. 2019 Presented at: 14th International Conference on Persuasive Technology; April 9, 2019; Limassol, Cyprus p. 43-45. [doi: [10.1007/978-3-030-17287-9](https://doi.org/10.1007/978-3-030-17287-9)]
3. Wilkowska W, Ziefle M. Privacy and data security in E-health: requirements from the user's perspective. *Health Informatics J* 2012 Sep 24;18(3):191-201 [FREE Full text] [doi: [10.1177/1460458212442933](https://doi.org/10.1177/1460458212442933)] [Medline: [23011814](https://pubmed.ncbi.nlm.nih.gov/23011814/)]
4. Pereira-Azevedo NM, Venderbos LDF. eHealth and mHealth in prostate cancer detection and active surveillance. *Transl Androl Urol* 2018 Feb;7(1):170-181. [doi: [10.21037/tau.2017.12.22](https://doi.org/10.21037/tau.2017.12.22)] [Medline: [29594031](https://pubmed.ncbi.nlm.nih.gov/29594031/)]
5. Yang W, Shah L, Spaulding E, Wang J, Xun H, Weng D, et al. The role of a clinician amid the rise of mobile health technology. *J Am Med Inform Assoc* 2019 Nov 01;26(11):1385-1388 [FREE Full text] [doi: [10.1093/jamia/ocz131](https://doi.org/10.1093/jamia/ocz131)] [Medline: [31373364](https://pubmed.ncbi.nlm.nih.gov/31373364/)]
6. van Gemert-Pijnen JEW, Nijland N, van Limburg M, Ossebaard HC, Kelders SM, Eysenbach G, et al. A holistic framework to improve the uptake and impact of eHealth technologies. *J Med Internet Res* 2011 Dec 05;13(4):e111 [FREE Full text] [doi: [10.2196/jmir.1672](https://doi.org/10.2196/jmir.1672)] [Medline: [22155738](https://pubmed.ncbi.nlm.nih.gov/22155738/)]
7. Editorial. Time to discuss consent in digital-data studies. *Nature* 2019 Aug;572(7767):5 [FREE Full text] [doi: [10.1038/d41586-019-02322-z](https://doi.org/10.1038/d41586-019-02322-z)] [Medline: [31367033](https://pubmed.ncbi.nlm.nih.gov/31367033/)]
8. Jochems A, Deist TM, van Soest J, Eble M, Bulens P, Coucke P, et al. Distributed learning: Developing a predictive model based on data from multiple hospitals without data leaving the hospital - A real life proof of concept. *Radiother Oncol* 2016 Dec;121(3):459-467 [FREE Full text] [doi: [10.1016/j.radonc.2016.10.002](https://doi.org/10.1016/j.radonc.2016.10.002)] [Medline: [28029405](https://pubmed.ncbi.nlm.nih.gov/28029405/)]
9. van Soest J, Sun C, Musmann O, Puts M, van den Berg B, Malic A, et al. Using the personal health train for automated and privacy-preserving analytics on vertically partitioned data. *Stud Health Technol Inform* 2018;247:581-585. [Medline: [29678027](https://pubmed.ncbi.nlm.nih.gov/29678027/)]
10. Chevrier R, Foufi V, Gaudet-Blavignac C, Robert A, Lovis C. Use and understanding of anonymization and de-identification in the biomedical literature: scoping review. *J Med Internet Res* 2019 May 31;21(5):e13484 [FREE Full text] [doi: [10.2196/13484](https://doi.org/10.2196/13484)] [Medline: [31152528](https://pubmed.ncbi.nlm.nih.gov/31152528/)]
11. Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun* 2019 Jul 23;10(1):3069. [doi: [10.1038/s41467-019-10933-3](https://doi.org/10.1038/s41467-019-10933-3)] [Medline: [31337762](https://pubmed.ncbi.nlm.nih.gov/31337762/)]
12. El Emam K, Rodgers S, Malin B. Anonymising and sharing individual patient data. *BMJ* 2015 Mar 20;350:h1139 [FREE Full text] [doi: [10.1136/bmj.h1139](https://doi.org/10.1136/bmj.h1139)] [Medline: [25794882](https://pubmed.ncbi.nlm.nih.gov/25794882/)]
13. Samarati P, Sweeney L. Protecting privacy when disclosing information: k-anonymityits enforcement through generalization and suppression. Data Privacy Lab De-identification Project.: Carnegie Mellon University; 2018. URL: <https://dataprivacylab.org/dataprivacy/projects/kanonymity/index3.html> [accessed 2021-02-23]

14. Sun C, Ippel L, van Soest J, Wouters B, Malic A, Adekunle O, et al. A privacy-preserving infrastructure for analyzing personal health data in a vertically partitioned scenario. *Stud Health Technol Inform* 2019 Aug 21;264:373-377. [doi: [10.3233/SHTI190246](https://doi.org/10.3233/SHTI190246)] [Medline: [31437948](https://pubmed.ncbi.nlm.nih.gov/31437948/)]
15. Netherlands Code of Conduct for Research Integrity 2018 [FREE Full text] [doi: [10.17026/dans-2cj-nvwu](https://doi.org/10.17026/dans-2cj-nvwu)]
16. Bonthuis MJ. 50 misverstanden over de Algemene Verordening Gegevensbescherming. Deventer, Netherlands: Wolters Kluwer; 2020.
17. App Checker. Royal Dutch Medical Association (KNMG). URL: <https://www.knmg.nl/advies-richtlijnen/knmg-publicaties/medische-app-checker.htm> [accessed 2019-11-18]
18. Kudina O, Verbeek P. Ethics from within: Google Glass, the Collingridge dilemma, and the mediated value of privacy. *Sci Technol Hum Values* 2018 Aug 21;44(2):291-314. [doi: [10.1177/0162243918793711](https://doi.org/10.1177/0162243918793711)]

Abbreviations

ECoWeB: emotional competence for well-being in the young

FAIR: Findable, Accessible, Interoperable, Reusable

GDPR: General Data Protection Regulation

Health-RI: Health Research Infrastructure Initiative

mHealth: mobile health

VSNU: Association of Universities in the Netherlands

Edited by G Eysenbach; submitted 13.12.19; peer-reviewed by N Seeman, DVS, M Abdelhamid; comments to author 30.03.20; revised version received 01.05.20; accepted 17.01.21; published 17.03.21

Please cite as:

Zegers CML, Witteveen A, Schulte MHJ, Henrich JF, Vermeij A, Klever B, Dekker A

Mind Your Data: Privacy and Legal Matters in eHealth

JMIR Form Res 2021;5(3):e17456

URL: <https://formative.jmir.org/2021/3/e17456>

doi: [10.2196/17456](https://doi.org/10.2196/17456)

PMID: [33729163](https://pubmed.ncbi.nlm.nih.gov/33729163/)

©Catharina M L Zegers, Annemieke Witteveen, Mieke H J Schulte, Julia F Henrich, Anouk Vermeij, Brigit Klever, Andre Dekker. Originally published in JMIR Formative Research (<http://formative.jmir.org>), 17.03.2021. This is an open-access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work, first published in JMIR Formative Research, is properly cited. The complete bibliographic information, a link to the original publication on <http://formative.jmir.org>, as well as this copyright and license information must be included.