Teaching Digital Health Ethics – Considerations and Lessons in Hands on Learning.

Arthi Kumaravel (✉ akumarav@bidmc.harvard.edu)
Beth Israel Deaconess Care Organization LLC
Philip Henson
Beth Israel Deaconess Care Organization LLC
John Torous
Beth Israel Deaconess Care Organization LLC

Research article

Keywords: GDPR, EU, HIPAA, digital privacy, resident education, smartphone applications, ethics, mhealth

Posted Date: February 11th, 2020

DOI: https://doi.org/10.21203/rs.2.23179/v1

Abstract

Background Educators need new tools to teach resident learners how to evaluate the privacy risks of and utilize the benefits of smartphone applications with their patients. To address this need for education addressing the changing landscape of mental health care delivery, we sought to create a simple tool that can be used in the clinic. Through this 10-point assessment framework for screening health apps based from ethical principles of the General Data Protection Regulation (GDPR), we propose a method that educators can utilize to teach residents about the privacy concerns of utilizing smartphone applications as part of clinical care with their patients. Methods We utilized an ethical-educational framework we developed from ethical principles of the GDPR with a group of 27 psychiatry residents from two academic centers for a simulation exercise to assess harms of using smartphone apps with a patient. Results All 27 raters completed the evaluations, but only 24 reported a time record for completion of the evaluation. The mean time to evaluate the privacy policy of the sample app's privacy policy was 434.2 seconds (just over five minutes). Percentage agreement of each question on the survey ranged from a high of 81.5% to a low of 48.1%. Conclusions In this study, we developed an assessment framework based on the ethical principles contained within the GDPR to utilize for education of resident learners around digital health privacy. This is the first framework developed for resident learners to help them understand the potential risks to patient privacy with the use of smartphone applications for mental health. The discussion prompted by an examination of a privacy policy through this framework highlights the need for further educational tools built into the residency education curriculum regarding these risks as use of these applications become more wide spread.

Background:

While mobile digital health technologies like smartphone apps offer the potential of increased access to innovative care in the near future, today many present concrete risks to patient privacy and a direct challenge to medical ethics [1]. This poses a new academic challenge of how to teach resident learners to be aware of and respond to these risks to patient privacy. Educators need new tools to teach resident learners how to evaluate the privacy risks of and utilize the benefits of smartphone applications with their patients. To fail to do so raises the risk of not preparing resident learners to be able to work effectively in a world with increasingly digitally based models of care delivery [2]. To address this need for education addressing the changing landscape of mental health care delivery, we sought to create a simple tool that can be used in the clinic. Through this 10-point assessment framework for screening health apps based from ethical principles of the General Data Protection Regulation (GDPR), we propose a method that educators can utilize to teach residents about the privacy concerns of utilizing smartphone applications as part of clinical care with their patients.

Patients are increasingly utilizing more self-help resources for their health, but residents are not trained to evaluate their safety or efficacy. In particular, one of the self-help resources patients are using increasingly is smartphone applications for their health [3]. There has been especially strong interest in mental health apps, likely because of the scarcity of mental health services in all countries around the world [4], yet less attention to training clinicians how to evaluate and use them. While this increase in patient interest to take charge of their own health through the use of technology offers many potential benefits, there are potential harms as well that both patients and clinicians need to be aware of and discuss.

One challenge for educators in teaching residents about digital technologies like apps is that these regulations are confusing and remain in flux. Although resident learners are currently in the age bracket of millennials and are “digital natives” in that they grew up utilizing technology both for education and pleasure [5], even they are not fully informed regarding the privacy policies and regulations in place for smartphone applications. In the United States, the vast majority of health apps exists outside of federal privacy protection (eg HIPAA) and instead uses their privacy policy to outline how patient’s personal health information is used, shared, or even marketed [6]. There is no federal law currently that regulates the collection and use of personal data. In Massachusetts, companies are required to encrypt any personal data that travels through public networks and California’s Consumer Privacy Act instills rules upon companies regarding clients’ data [7]. While educators are not expected to be health technology policy experts, it is clear that teaching residents to use technology in a safe and effective manner will require a focus on higher level principles that will offer relevant guidance regardless of changes in policy. Such higher-level principles must be ethical guidance, which can offer clear direction even in the face of rapidly changing technology, policy, and regulation. Considering this new competency area for mobile health and smartphone apps grounded in integrity and ethical behavior well aligns with existing professional development frameworks for psychiatry education [8]. Practical and clinically actionable skills for ethical behavior with regards to smartphone apps include being able to “weigh the pros and cons of use and data transfer with clinical and ethical principles” [8]. The methods to teach these core competencies include didactic and case-based learning and below we present a case-based approach.

We developed a framework derived from ethical principles contained within the General Data Protection Regulation, (GDPR) as it offers to most concrete guidance in the world today around digital health. The GDPR [8], ratified in May 2018 by the European Union (EU), outlines a set of data protection rules for all companies that operate or have clients in the EU, regardless of primary base of operations [10]. The GDPR will be enforced by the Information Commissioner’s Office and requires that companies obtain consent from clients prior to collection of personal data, allow clients access to the data and the ability to delete or modify their data [11]. Failure to comply with the regulations can lead to a fine of “4 percent of a company’s annual global revenue” [11]. Due to the fiscal penalties of noncompliance with the GDPR, there now exists a method of enforcement to ensure consumer privacy and thus a tangible target to align digital health teaching towards.

Methods:

We utilized an ethical-educational framework we developed from ethical principles of the GDPR with a group of 27 psychiatry residents from two academic centers for a simulation exercise to assess harms of using smartphone apps with a patient.

Development and implementation of ethical framework for app assessment:

Each article of the GDPR was reviewed for ethical principles specifically pertaining to teachable patient and clinician factors as to be most relevant for evaluation of apps for clinical use by two of the authors (AK and JT). After review, chapter 1 article 1, chapter 2 article 6, chapter 3, articles 12, 13, 17 and 21, and chapter 4 articles 32, 33 and 34 were found to have the most concrete, teachable, and clinically relevant ethical principles for assessment of apps. The specific excerpts from these articles were linked with their underlying ethical principles. Questions for app evaluation that learners and educators could use were developed to correlate with ethical principles. See Table 1.

Search criteria and selection:

Pacifica for Stress & Anxiety app was selected as a sample smartphone app for resident utilization of the validated framework. This application was downloaded from the Apple iTunes Store on November 1st, 2018, along with the most current version of the privacy policy at that date.

App assessment:

After obtaining IRB permission, 27 psychiatry residents from two residency programs were given the previously validated framework developed from the GDPR to assess for a sample app's privacy policy. The smartphone application selected as a sample study was Pacifica for Stress & Anxiety. The survey was completed on November 21, 2018 as part of an educational lecture on privacy policies of smartphone apps. Residents were asked to time themselves in order to assess how much time burden app evaluation may take in care settings.

Statistical analysis:

Mean agreement in response to each question between each rater was determined by obtaining an average of the responses provided by each of the 27 raters per question. For our study, percent agreement greater than 70% was determined to be strong agreement, 50 to 70% as good agreement and between 30 and 50% as moderate agreement and less than 30% as weak agreement.

Results:

All 27 raters completed the evaluations, but only 24 reported a time record for completion of the evaluation. The mean time to evaluate the privacy policy of the sample app's privacy policy was 434.2 seconds (just over five minutes). Percent agreement for each of the questions is displayed in Figure 1.

Discussion:

In this study, we developed the first ethical framework developed to teach resident learners about ethical use of smartphone apps in practice. Simulation and case-based learning is important in engaging adult learners and helping them develop practical skills. In this exercise, we wished to help psychiatry residents utilize a framework with which to discuss the risks of using smartphone applications for mental health with their patients and to open the discussion regarding any concerns or difficulties they may have already faced in the clinic and how this framework could mitigate some of those difficulties.

As described previously, the GDPR provides a foundation for the development of a set of guidelines derived from actionable ethical principles. In thinking about how resident learners not only understand and develop their professionalism and the core competency of ethical care, it is important they engage in hands on and relevant learning as this simulation offered. This simulation offers the initial steps of working with for resident learners in how to discuss and document the risks of smartphone applications as part of a treatment for a patient.

The findings from the utilization of the framework highlights its applicability around the applicability of the ethical principles in this setting. Question number 2, “Are the risks outlined in an easy to understand format?”, which examines the ethical principle of informed consent, afforded the highest percentage of agreement at 81.5%. It is not surprising then that a group of learners with mindfulness towards patient care with prior training regarding the risks and benefits of various treatments would be most attuned to this question. Question 6, “Does this app have systems in place to protect client’s personal data with regards to transfer of their personal data?”, focusing on the ethical principle of respect for persons, examines whether the app has systems in place to protect a client’s data. This question had the lowest percentage of agreement, highlight an important need for educators to address. The question touches upon the technological systems in place for data protection, suggesting that more education regarding the types of systems that can be in place are necessary before an evaluation of privacy policies for certain standards can be completely utilized with patients.

In the discussion following the case-based simulation exercise, several themes were raised that indicate areas of further study and need for develop of educational areas for resident learners regarding this topic. The included the lack of prior rigorous studies of the risks of smartphone apps and the lack of guidelines felt by psychiatry residents. Additional concerns were raised regarding the vague language used in the privacy policy itself, the inference of what risk is and informed consent as related to medical treatments versus consumerism and the need for asking about app use in practice with patients as a standard practice.

Limitations of the exercise include long length of time for completion of the framework at just over five minutes, suggesting that more didactic teaching may have been necessary prior to case-based learning of these complex ethical concepts. Even in a digitally native cohort of psychiatry residents, there were challenges in addressing the nature of the risks and addressing informed consent with patients regarding smartphone apps. This highlights the need for further teaching modules and education regarding the risks of mobile health as well as the need for more research in this area to understand the nature of the risks.

Conclusion:

In this study, we developed an assessment framework based on the ethical principles contained within the GDPR to utilize for education of resident learners around digital health privacy. This is the first framework developed for resident learners to help them understand the potential risks to patient privacy with the use of smartphone applications for mental health. The discussion prompted by an examination of a privacy policy through this framework highlights the need for further educational tools built into the residency education curriculum regarding these risks as use of these applications become more wide spread.

Declarations

- Ethics approval and consent to participate: IRB at Beth Israel Deaconess Medical Center (IRB exemption approved).
- Consent for publication: Consent verbally obtained from study participants after IRB waived need for written consent.
- Availability of data and materials: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.
- Competing interests: On behalf of all authors, the corresponding author states that there is no conflict of interest
- Funding: none
- Authors' contributions:
    - AK and JT designed the framework questions based from the GDPR. AK presented the simulation experience and distributed the framework for app analysis and contributed the majority of the writing of the manuscript. PH and JT did the statistical analysis for the data. All authors read and approved the final manuscript.
- Acknowledgements: none

References:

1. Roberts LW, Torous J. Preparing residents and fellows to address ethical issues in the use of mobile technologies in clinical psychiatry. Acad Psychiatry. 2017;41:132–4.
2. Torous, J., Chan, S., Luo, J. et al. Acad Psychiatry (2018) 42: 694. https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/s40596-017-0811-4
3. The Lancet Psychiatry Commission *Lancet Psychiatry*4 (2017): 775–818.
4. Torous, J., Roberts L.W., “The Ethical Use of Mobile Health Technology in Clinical Psychiatry,*”The Journal of Nervous and Mental Disease* 205 (2017): 4-8.

5. Zalpuri, I., Liu, H.Y., Stubbe, D. et al. Acad Psychiatry (2018) 42: 808. https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/s40596-018-0983-6
6. DeSalvo K. B., Samuels J., "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated By HIPAA," *Privacy and Security of EHRs*, July 19, 2016.
7. John, L. K., "Uninformed Consent," *Harvard Business Review*, September 2018.
8. Hilty, Donald M, et al. "Mobile Health, Smartphone/Device, and Apps for Psychiatry and Medicine Competencies, Training, and Faculty Development Issues." Psychiatr Clin North Am.2019 Sep;42(3):513-534.
9. 2018 reform of EU data protection rules, European Commission, August 2018,https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
10. General Data Protection Regulations (GDPR),https://gdpr-info.eu/.
11. Fung, B., "Why you're getting flooded with privacy notifications in your email," *The Switch Analysis*, May 25, 2018.

Table

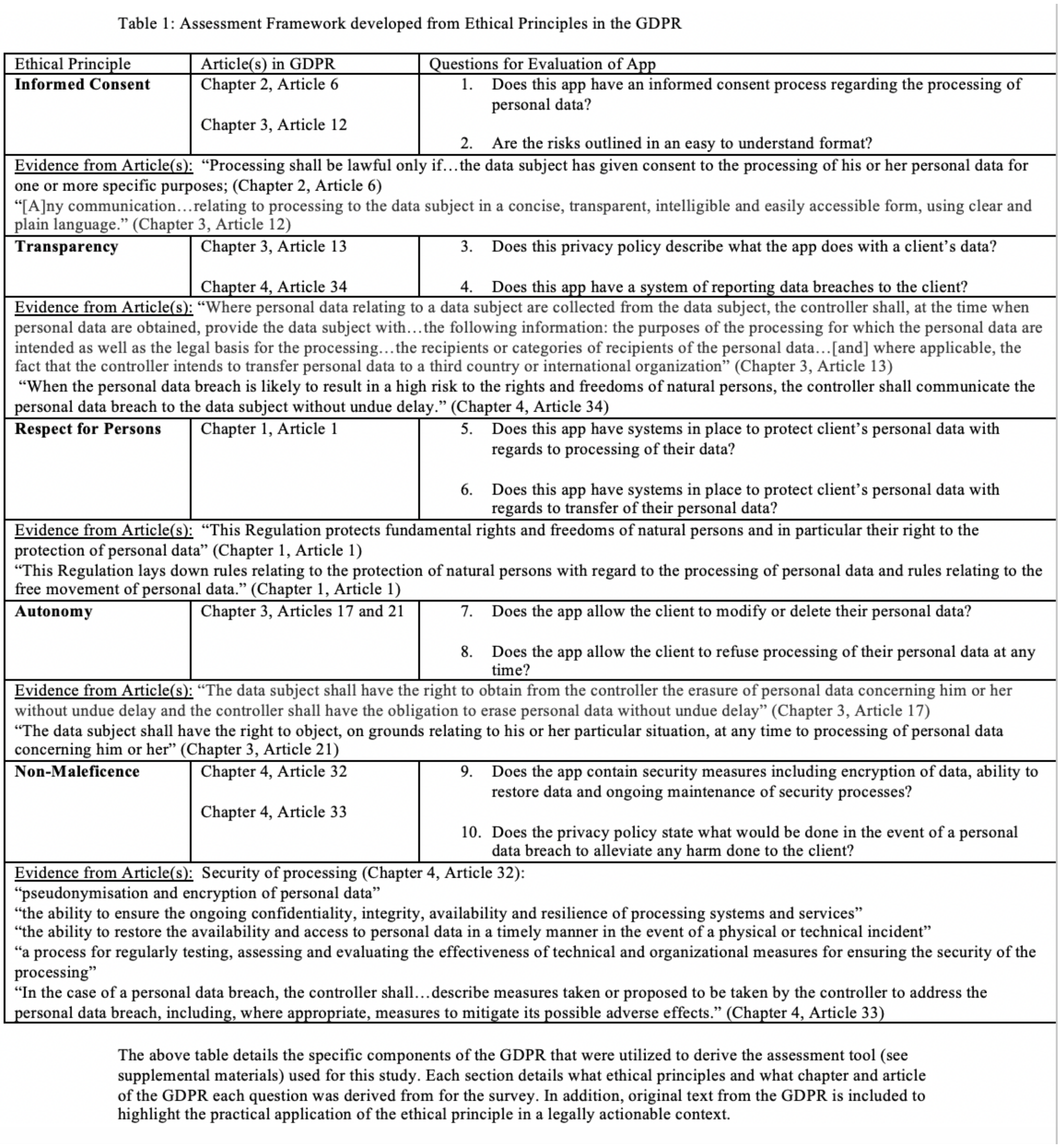

Table 1: Assessment Framework developed from Ethical Principles in the GDPR

Ethical Principle	Article(s) in GDPR	Questions for Evaluation of App
Informed Consent	Chapter 2, Article 6 Chapter 3, Article 12	1. Does this app have an informed consent process regarding the processing of personal data? 2. Are the risks outlined in an easy to understand format?
Evidence from Article(s): "Processing shall be lawful only if…the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (Chapter 2, Article 6) "[A]ny communication…relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language." (Chapter 3, Article 12)		
Transparency	Chapter 3, Article 13 Chapter 4, Article 34	3. Does this privacy policy describe what the app does with a client's data? 4. Does this app have a system of reporting data breaches to the client?
Evidence from Article(s): "Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with…the following information: the purposes of the processing for which the personal data are intended as well as the legal basis for the processing…the recipients or categories of recipients of the personal data…[and] where applicable, the fact that the controller intends to transfer personal data to a third country or international organization" (Chapter 3, Article 13) "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay." (Chapter 4, Article 34)		
Respect for Persons	Chapter 1, Article 1	5. Does this app have systems in place to protect client's personal data with regards to processing of their data? 6. Does this app have systems in place to protect client's personal data with regards to transfer of their personal data?
Evidence from Article(s): "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (Chapter 1, Article 1) "This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data." (Chapter 1, Article 1)		
Autonomy	Chapter 3, Articles 17 and 21	7. Does the app allow the client to modify or delete their personal data? 8. Does the app allow the client to refuse processing of their personal data at any time?
Evidence from Article(s): "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" (Chapter 3, Article 17) "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her" (Chapter 3, Article 21)		
Non-Maleficence	Chapter 4, Article 32 Chapter 4, Article 33	9. Does the app contain security measures including encryption of data, ability to restore data and ongoing maintenance of security processes? 10. Does the privacy policy state what would be done in the event of a personal data breach to alleviate any harm done to the client?
Evidence from Article(s): Security of processing (Chapter 4, Article 32): "pseudonymisation and encryption of personal data" "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident" "a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing" "In the case of a personal data breach, the controller shall…describe measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects." (Chapter 4, Article 33)		

The above table details the specific components of the GDPR that were utilized to derive the assessment tool (see supplemental materials) used for this study. Each section details what ethical principles and what chapter and article of the GDPR each question was derived from for the survey. In addition, original text from the GDPR is included to highlight the practical application of the ethical principle in a legally actionable context.

Figures

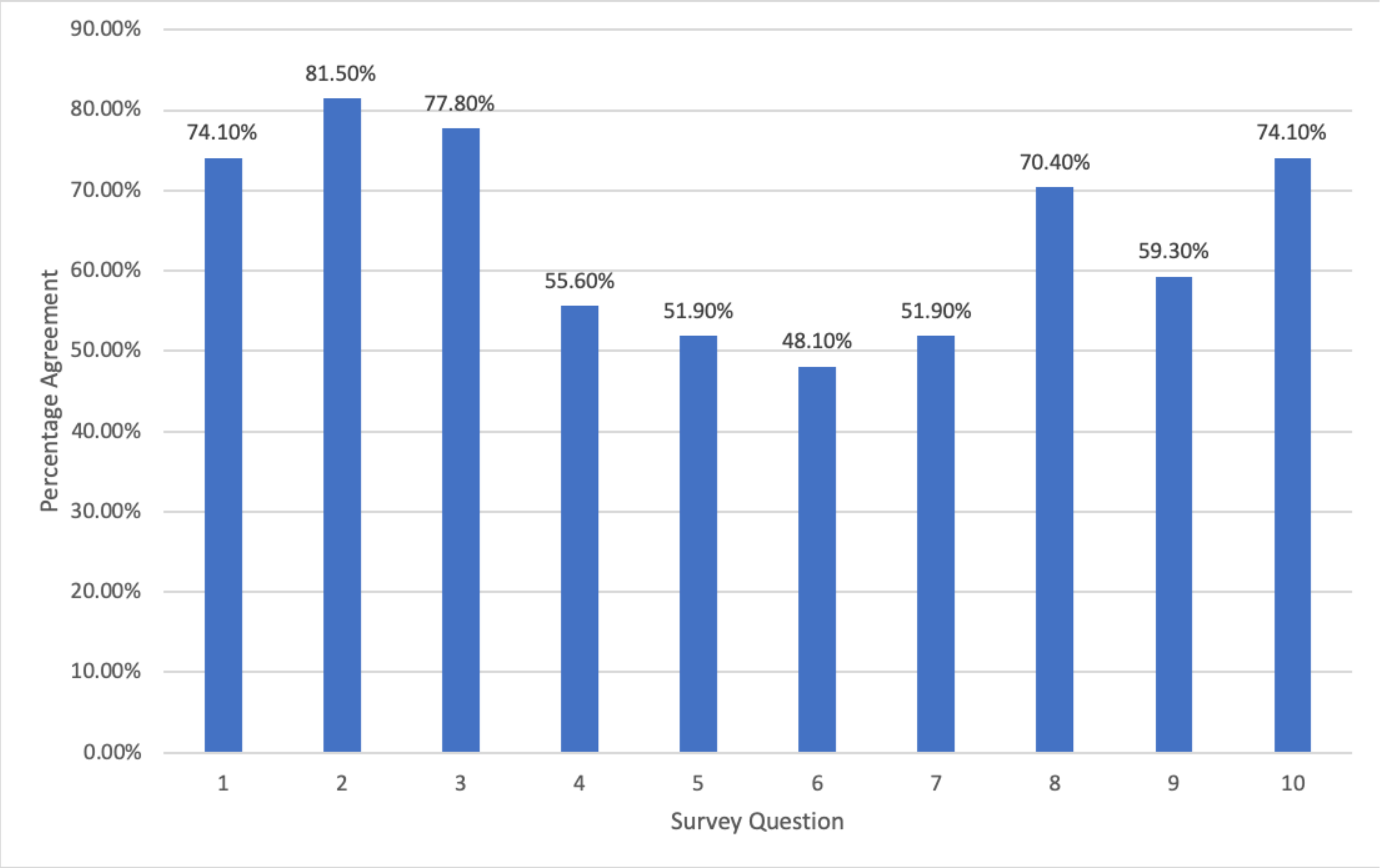

Figure 1

Percentage Agreement Per Survey Question. Displayed above are the percentage agreement between study participants per question answering a binary yes or no per question. Questions 1 and 2 address informed consent. 1) Does this app have an informed consent process regarding the processing of personal data? 2) Are the risks outlined in an easy to understand format? Questions 3 and 4 address transparency. 3) Does this privacy policy describe what the app does with a client's data? 4) Does this app have a system of reporting data breaches to the client? Questions 5 and 6 address respect for persons. 5) Does this app have systems in place to protect client's personal data with regards to processing of their data? 6) Does this app have systems in place to protect client's personal data with regards to transfer of their personal data? Questions 7 and 8 address autonomy. 7) Does the app allow the client to modify or delete their personal data? 8) Does the app allow the client to refuse processing of their personal data at any time? Questions 9 and 10 address non-maleficence. 9) Does the app contain security measures including encryption of data, ability to restore data and ongoing maintenance of security processes? 10) Does the privacy policy state what would be done in the event of a personal data breach to alleviate any harm done to the client?

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SupplementalFigure.docx