Case Study

Research Ethics
1–9

DOI: 10.1177/1747016120980560
journals.sagepub.com/home/rea
SAGE

Community-based health care providers as research participant recruitment gatekeepers: ethical and legal issues in a real-world case example

Karen L Celedonia
Turku University Hospital and University of Turku, Finland; Pressley Ridge, USA

Michael W Valenti
Pressley Ridge, USA

Marcelo Corrales Compagnucci
University of Copenhagen, Denmark

Michael Lowery Wilson
University of Heidelberg, Germany

Abstract

Community-based mental health care providers (CBMHCPs) are increasingly contacted by external researchers for research study recruitment. Unfortunately, many do not possess the resources or personnel with the skills required to successfully evaluate research proposals for risks. Providing access to clients and client health information can result in harmful personal and legal consequences if the proper safeguards do not exist. This article discusses the legal requirements and practical implications for CBMHCPs when acting as gatekeepers.

Corresponding author:
Michael Lowery Wilson, Heidelberg Institute of Global Health (HIGH), University of Heidelberg, Neuenheimer Feld 130.3, Heidelberg 69117, Germany.
Email: michael.wilson@uni-heidelberg.de

A case study from a large CBMHCP is presented as an illustration of steps that can be taken to protect clients and avoid risk. Additional recommendations for establishing protective safeguards and research evaluation protocols are discussed.

Keywords
Recruitment, community-based providers, partnership, mental health, guidelines, recommendations

Gatekeepers: a real-world case example

In an effort to generate findings that are more translatable, universities and other research institutions are increasingly approaching community-based health care providers (CBMHCPs) to request access to their clients for participation in research (Weinrich et al., 1998). While the desire to produce generalizable results that are representative of real-world populations seems at face-value to be sound, this can pose ethical and legal challenges if the CBMHCP does not have the expertise to critically assess the nature and ethics of the research. In particular, whether the research participants' rights and privacy are adequately protected and in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States (US) or the General Data Protection Regulation (GDPR) (CDC, 2019; European Union, 2019) in the European Union (EU).

The present case study was carried out in the United States and hence, relevant for American institutions collecting data on persons resident in the US. However, the European GDPR legislation also applies to American institutions who collect personal data from European citizens via the Internet. If this information is not stored properly, a data breach could violate the research subjects' privacy (Myers et al., 2008). The case is illustrative of the potential vulnerability of CBMHCPs and the ethical and legal issues that may arise when approached by an external research entity.

Pressley Ridge is a multi-site, multi-service CBMHCP based in Pittsburgh, Pennsylvania. The organization is frequently approached by local universities for recruitment of clients as research participants. While the majority of research proposals Pressley Ridge receives from external researchers involve low risk research activities such as using secondary data or participation in surveys, occasionally a study will involve activities of a higher risk nature, such as testing a medical device or other new health care technology. One such study was recently reviewed. The external researcher wanted to recruit participants from the organization to test a wearable electronic device that tracked children who exhibit wandering behavior.

Unlike most CBMHCPs, Pressley Ridge has the infrastructure to critically evaluate research presented by external entities; an entire department comprised of master's and doctoral level employees with decades of research experience exists

within the organization. There is also a dedicated Research Review Committee[1] and an organization-wide policy and protocol for responding to and evaluating external research proposals. Members of the Research Review Committee use the standardized protocol to (a) evaluate whether prospective studies pose any risks to potential research participants, and (b) estimate the potential burden participating in the study may exact on the organization. Pressley Ridge's protocol also includes guidelines for the use of critical paperwork associated with conducting research such as informed consent letters, rights of refusal (for staff and clients), and HIPAA authorization forms. The issues considered in relation to this application related primarily to the processing of sensitive personal data. Review of such activities requires knowledge and understanding of the applicable regulatory frameworks.

Protection of privacy

HIPAA is a federal law in the US that required the creation of national standards to protect sensitive health data from being disclosed without consent. The HIPAA Privacy Rule established national standards to protect individual level identifiable information (called "protected health information" (PHI)) (Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule, 2009; Wu, 2007). The HIPAA Security Rule operationalizes the protection included in the HIPAA Privacy Rule by addressing the technical and non-technical requirements that organizations must implement to protect individual health data. This Rule protects a subset of information covered by the HIPAA Privacy Rule which relates to all individually identifiable information which is processed in electronic form (called "electronic protected health information" (e-PHI)). The HIPAA Security Rule must be adopted by three main types of healthcare organizations: (a) healthcare providers, (b) health plans, and (c) healthcare clearinghouses that process health data by electronic means.

The rise of digitalization and new mobile technologies such as medical apps and cloud-based electronic health records have increased data security risks (Compagnucci et al., 2019). One of the primary goals of the HIPAA Security Rule is to protect individual privacy, in particular while implementing new technologies that are intended to improve the quality and efficiency of patient care. The HIPAA Security Rule was designed to be flexible and scalable, to ensure the coverage of a wide range of technologies relevant to the organization's size, structure, and risks to patients' health data (Office for Civil Rights (OCR), 2009). The administrative safeguards provisioned in the HIPAA Security Rule call for health care organizations to perform a risk analysis as part of their security management processes. The risk analysis and management provisions enshrined in the HIPAA Security Rule are highlighted in this paper in order to raise awareness of the security and organizational measures that healthcare organizations need to take into

account. By and large, a risk analysis process includes, but it is not limited to, the following steps: (a) evaluate the likelihood of its occurrence and impact of potential electronic protected health information (e-PHI), (b) implement appropriate security measures to address the risks identified in the risk analysis, (c) document the chosen security measures and, where required, the rationale for adopting those measures, and (d) maintain continuous, reasonable, and appropriate security protections (Leo, 2004; OCR, 2009; Talabis and Martin, 2012).

The GDPR in Europe has a more general scope but also covers health data. According to the GDPR, a Data Protection Impact Assessment (DPIA) should be carried out before processing of personal data that is likely to involve "a high risk" (Wolford, 2019). According to Article 35 of the GDPR, a DPIA must be conducted "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data." Risk in this context refers to the potential for any significant physical, material or non-material harm to individuals. For assessment of whether risks are high, the GDPR recommends consideration of both the likelihood and severity of any potential harm to individuals. A "high risk" implies a higher threshold than a remote chance of some harm, either because the harm is more likely to occur, or because the potential harm is more severe, or a combination of the two (ICO, 2020; Voigt and Von dem Bussche, 2017). While the majority of research proposals Pressley Ridge receives from external researchers involve low risk research activities such as using secondary data or collecting surveys, occasionally a study will involve activities of a higher risk nature, such as testing a medical device or other new health care technology. One such study was recently evaluated by the Research Review Committee. The external researcher wanted to recruit participants from the organization to test a wearable electronic device that tracked children who exhibit wandering behavior.

The GDPR is rigorous with regard to the use of new technologies and the tracking of people's location or behavior. Additionally, there are precise requirements regarding the processing of personal and sensitive data (in particular, children's data), systematically monitoring a publicly accessible place on a large scale, and automated decision-making about people that could have legal (or similarly significant) consequences. In all these situations, a DPIA is required to help identify and mitigate the risks of data breaches and to ensure that data protection and security standards are met (Storr and Storr, 2017; Wrigley, 2018).

In Europe, the Article 29 Working Party published guidelines with nine criteria for assessing whether data processing is likely to result in high risk. These criteria are as follows: (1) Evaluation or scoring; (2) Automated decision-making with legal or similar significant effect; (3) Systematic monitoring; (4) Sensitive data or

data of a highly personal nature; (5) Data processed on a large scale; (6) Matching or combining datasets; (7) Data concerning vulnerable data subjects; (8) Innovative use or applying new technological or organizational solutions; and (9) Preventing data subjects from exercising a right or using a service or contract (Mondschein and Monda, 2019; Party, 2017). In most circumstances, a combination of two of these factors indicates the need for a DPIA. However, this is not a strict rule.

With regard to the proposed study for tracking children who wander, more than two of these factors were present which highlights the high-risk nature of the proposed project (ICO, 2020). Though not physically invasive, wearable electronic devices pose a level of privacy invasion. The data collected by these devices is often personal, includes sensitive, health-related information, and should be safeguarded as such. The involvement of children adds a further degree of sensitivity and risk. In addition, most personal health data generated by commercially available wearable electronic devices (i.e. Fitbit) are "transferred to entities outside the control of the data producer, including the device's manufacturer or a third party" (Diaz et al., 2015; Spann, 2015).

Even when developed for non-commercial reasons, details about what data is collected, how it is used, stored and transferred would need to be provided in order to assess how the end-users' rights and privacy are being considered. Appropriate data storage and protection procedures are among the main concerns for an institutional review board (IRB). Hence, one might assume that if a study has obtained IRB approval that the proposed data storage and protection procedures have been judged as sufficient and in compliance with regulatory requirements. If a CBMHCP lacks the knowledge and expertise to critically evaluate risks, prior approval from an IRB might (reasonably) be enough for the organization to allow the research to proceed.

Indeed, in this case example, the principal investigator (PI) had provided Pressley Ridge's Research Review Committee with an approval letter from their institution's IRB, as well as research recruitment materials. However, they did not provide any details regarding data collection and storage/protection. Given that the Research Review Committee is comprised of seasoned master's and doctorate level researchers, this lack of information raised a 'red flag', and more information regarding data storage and protection was requested from the PI before a final decision could be taken regarding the risk level of the study. The PI never responded to this request, and the study was ultimately denied access to Pressley Ridge's clients for recruitment.

Lessons learned and recommendations

CBMHCPs are first and foremost providers of care to their clients; their main priority is the well-being and safety of the people they serve. However, CBMHCPs

are increasingly finding themselves in the role of gatekeepers to research institutes who request special access to their clients for study recruitment. Should access be granted for recruitment and then a violation of privacy occur, it is not only the PI who will be held responsible for this transgression, but the CBMHCP as well. CBMHCP clients trust that their providers have their best interests at heart and are looking out for them. To wantonly allow external researchers to recruit from the organization's client base could be viewed as an abuse of this trust, or worse, a complete disregard of the client-provider relationship.

The ethical and legal issues surrounding wearable devices are delicate and they deserve closer consideration. Medical apps for research are increasingly popular tools for gathering and analyzing data for clinical research studies in a more efficient and automated fashion. However, CBMHCPs have duties related to a fiduciary relationship with their clients. If there are accidents such as data leaks, the participants or family members can bring a lawsuit based on two common grounds of reasoning: (a) breach of contract; or (b) negligence. In most circumstances, the court finds it easier to file the legal claim on the grounds of medical negligence. Relevant staffing expertise can reduce the uncertainties and reduce the information gap between the involved parties (Compagnucci, 2020).

For the case example described in this paper the outcome might have been very different had the organization not had the requisite resources and expertise to critically evaluate the research proposal presented by the external research institute and access may have been granted without further questioning of the protocol. This raises the question of what are CBMHCPs without the relevant resources and expertise to do when approached by external research entities? One cannot expect every CBMHCP to have a department devoted to research and evaluation, but certain steps can be taken to ensure that clients are not exposed to unnecessary risk if they consent to participate in a study. The simplest course of action might be the development of a standard operating procedure (SOP) for responding to requests, along the lines that Pressley Ridge has established.

The Research Review Committee at Pressley Ridge uses a standard evaluation form to assess risks to potential participants and staff members. This form asks reviewers to consider the following in regards to the proposed research: (a) if the participants' rights are protected, (b) if the participant can refuse to participate without consequences, (c) if consent is freely given, specific, informed and unambiguous, (d) the value of the research in regards to understanding mental health disorders, (e) the value of research to improving treatment for individuals with mental health disorders, (f) the value of the research to informing evidence-based practice, and (g) the effort required of the organization's staff to participate in the research.

After the reviewer has considered these seven areas, they are then asked to make a final decision on whether or not to allow the external research access to the organization's clients. Decisions are categorized as: (a) approved—exempt,

without concerns, (b) approval—non-exempt, risk identified, and (c) rejected. If a study is identified as having minimal risk, it is passed on to the senior leadership level for further evaluation and decision upon whether to grant access to the organization's clients.

The development of an SOP does not need to be particularly time intensive or demanding for the CBMHCP's staff. At most, it would require a few meetings to discuss and finalize the SOP. The addition of a Research Review Committee could be considered to implement the SOP. If there are no research professionals on staff at the organization, composition of the committee could include senior leadership, existing clients, and interested staff. Access to training and continuing education via journal articles, research-themed webinars or other classes could help with skills development. If the organization has the financial means, a research professional could be kept on retainer for consultation as needed.

Once a SOP for responding to research requests is developed, organizational leadership must ensure that the SOP is shared with and understood by all program leaders. At Pressley Ridge, most external research requests are received directly by program or service managers, not by members of the Research Review Committee. Without effective communication of the organization's protocols and procedures, uninformed service managers may provide access to clients or protected health information without evaluating risks.

Conclusion

The inclusion of CBMHCPs in studies conducted by external research institutions can be a rewarding experience for both parties. However, if the CBMHCP lacks the resources and expertise to critically assess and evaluate research protocols, clients may be exposed to unnecessary risks should they choose to participate in research. Steps should be taken to ensure that access to clients is granted only after careful review and evaluation of research protocols and potential risks.

Funding

All articles in Research Ethics are published as open access. There are no submission charges and no Article Processing Charges as these are fully funded by institutions through Knowledge Unlatched, resulting in no direct charge to authors. For more information about Knowledge Unlatched please see here: http://www.knowledgeunlatched.org.

ORCID iD


Michael Lowery Wilson https://orcid.org/0000-0002-4007-3496

Note

1. Two authors of this paper are employed by Pressley Ridge and sit on the Research Review Committee.

References

CDC (2019) Health insurance portability and accountability act of 1996 (HIPAA). Available at: https://www.cdc.gov/phlp/publications/topic/hipaa.html (accessed 16 November 2020).

Compagnucci MC (2020) *Big Data, Databases and "Ownership" Rights in the Cloud*. Springer.

Compagnucci MC, Meszaros J, Minssen T, et al. (2019) *Homomorphic encryption: The 'holy grail' for big data analytics & legal compliance in the pharmaceutical and healthcare sector?* ID 3488291, SSRN Scholarly Paper, 15 November. Rochester, NY: Social Science Research Network. Available at: https://papers.ssrn.com/abstract=3488291 (accessed 16 November 2020).

Diaz KM, Krupka DJ, Chang MJ, et al. (2015) Fitbit®: An accurate and reliable device for wireless physical activity tracking. *International Journal of Cardiology* 185: 138–140.

European Union (2019) EUR-Lex: 32016R0679. Available at: https://eur-lex.europa.eu/legal-content/EN-NL/TXT/?uri=CELEX%3A32016R0679 (accessed 16 November 2020).

ICO (2020) When do we need to do a DPIA? Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/ (accessed 16 November 2020).

Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule (2009) Beyond the HIPAA privacy rule: Enhancing privacy, improving health through research. In: Nass SJ, Levit LA and Gostin LO (eds) *The National Academies Collection: Reports Funded by National Institutes of Health*. Washington, DC: National Academies Press (US). Available at: http://www.ncbi.nlm.nih.gov/books/NBK9578/ (accessed 16 November 2020).

Leo RA (2004) *The HIPAA Program Reference Handbook*. Boca Raton, FL: CRC Press.

Mondschein CF and Monda C (2019) The EU's general data protection regulation (GDPR) in a research context. In: Kubben P, Dumontier M and Dekker A (eds) *Fundamentals of Clinical Data Science*. Cham: Springer, 55–71.

Myers J, Frieden TR, Bherwani KM, et al. (2008) Ethics in public health research: Privacy and public health at risk: Public health confidentiality in the digital age. *American Journal of Public Health* 98(5): 793–801.

Office for Civil Rights (OCR) (2009) Summary of the HIPAA security rule. Available at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html?language=en (accessed 16 November 2020).

Party DPW (2017) Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679.

Spann S (2015) Wearable fitness devices: Personal health data privacy in Washington state. *Seattle University Law Review* 39: 1411.

Storr C and Storr P (2017) Internet of things: Right to data from a European perspective. In: *New Technology, Big Data and the Law*. Singapore: Springer, 65–96.

Talabis M and Martin J (2012) *Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis*. Newnes.

Voigt P and Von dem Bussche A (2017) *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 1st edn. Cham: Springer International Publishing.

Weinrich SP, Boyd MD, Bradford D, et al. (1998) Recruitment of African Americans into prostate cancer screening. *Cancer Practice* 6(1): 23–30.

Wolford B (2019) What is a GDPR data processing agreement? Available at: https://gdpr.eu/what-is-data-processing-agreement/ (accessed 16 November 2020).

Wrigley S (2018) Taming artificial intelligence: "Bots," the GDPR and regulatory approaches. In: Corrales M, Fenwick M and Forgó N (eds) *Robotics, AI and the Future of Law*. Springer, 183–208.

Wu SS (2007) *A Guide to HIPAA Security and the Law*, 2nd edn. Chicago, IL: ABA Book Publishing. Available at: https://www.americanbar.org/products/inv/book/253309969/ (accessed 16 November 2020).