Canadian Journal of Bioethics
Revue canadienne de bioéthique

Canadian Journal of Bioethics
Revue Canadienne de Bioéthique

Research, Digital Health Information and Promises of Privacy: Revisiting the Issue of Consent

Timothy Caulfield, Blake Murdoch and Ubaka Ogbogu

Volume 3, Number 1, 2020

URI: https://id.erudit.org/iderudit/1070237ar
DOI: https://doi.org/10.7202/1070237ar

See table of contents

Publisher(s)

Programmes de bioéthique, École de santé publique de l'Université de Montréal

ISSN

2561-4665 (digital)

Explore this journal

Cite this article

Caulfield, T., Murdoch, B. & Ogbogu, U. (2020). Research, Digital Health Information and Promises of Privacy: Revisiting the Issue of Consent. *Canadian Journal of Bioethics / Revue canadienne de bioéthique*, *3*(1), 164–171. https://doi.org/10.7202/1070237ar

Article abstract

The obligation to maintain the privacy of patients and research participants is foundational to biomedical research. But there is growing concern about the challenges of keeping participant information private and confidential. A number of recent studies have highlighted how emerging computational strategies can be used to identify or reidentify individuals in health data repositories managed by public or private institutions. Some commentators have suggested the entire concept of privacy and anonymity is “dead”, and this raises legal and ethical questions about the consent process and safeguards relating to health privacy. Members of the public and research participants value privacy highly, and inability to ensure it could affect participation. Canadian common law and legislation require a full and comprehensive disclosure of risks during informed consent, including anything a reasonable person in the participant or patient’s position would want to know. Research ethics policies require similar disclosures, as well as full descriptions of privacy related risks and mitigation strategies at the time of consent. In addition, the right to withdraw from research gives rise to a need for ongoing consent, and material information about changes in privacy risk must be disclosed. Given the research ethics concept of “non-identifiability” is increasingly questionable, policies based around it may be rendered untenable. Indeed, the potential inability to ensure anonymity could have significant ramifications for the research enterprise.

Canadian Journal of Bioethics
Revue canadienne de bioéthique

T Caulfield, B Murdoch, U Ogbogu. *Can J Bioeth / Rev Can Bioeth.*
2020;3(1):164-171

ARTICLE (ÉVALUÉ PAR LES PAIRS / PEER-REVIEWED)

Research, Digital Health Information and Promises of Privacy: Revisiting the Issue of Consent

Timothy Caulfield[1], Blake Murdoch[1], Ubaka Ogbogu[1]

Résumé
L'obligation de préserver la vie privée des patients et des participants à la recherche est fondamentale en recherche biomédicale. Toutefois, les défis à relever pour maintenir la confidentialité des informations sur les participants suscitent une inquiétude croissante. Un certain nombre d'études récentes a mis en évidence les manières d'utiliser les nouvelles stratégies informatiques pour identifier ou réidentifier les personnes dans les banques de données de santé gérées par des institutions publiques ou privées. Certains commentateurs ont laissé entendre que les concepts de vie privée et d'anonymat sont "morts" dans leur ensemble, ce qui soulève des questions juridiques et éthiques sur le processus de consentement et sur les garanties relatives à la protection de la vie privée en matière de santé. Les membres du public et les participants à la recherche accordent une grande importance à la protection de la vie privée, et l'incapacité à garantir celle-ci pourrait avoir une incidence sur la participation. La common law et la législation canadienne exigent une divulgation complète et exhaustive des risques lors du consentement éclairé, y compris tout ce qu'une personne raisonnable dans la position du participant ou du patient voudrait savoir. Les politiques en matière d'éthique de la recherche exigent des divulgations similaires, ainsi que des descriptions complètes des risques liés à la vie privée et des stratégies d'atténuation lors du consentement. En outre, le droit de se retirer de la recherche entraîne la nécessité d'un consentement continu, et toute information sur l'évolution du risque pour la vie privée doit être divulguée. Étant donné que le concept de "non-identifiabilité" en matière d'éthique de la recherche est de plus en plus discutable, les politiques qui s'y rattachent pourraient devenir intenables. En effet, l'incapacité potentielle à garantir l'anonymat pourrait avoir des conséquences importantes sur l'activité de recherche.

Mots-clés
vie privée, confidentialité, consentement éclairé, informations sur la santé, biobanques, identifiabilité, éthique de la recherche, droit de la santé

Abstract
The obligation to maintain the privacy of patients and research participants is foundational to biomedical research. But there is growing concern about the challenges of keeping participant information private and confidential. A number of recent studies have highlighted how emerging computational strategies can be used to identify or reidentify individuals in health data repositories managed by public or private institutions. Some commentators have suggested the entire concept of privacy and anonymity is "dead", and this raises legal and ethical questions about the consent process and safeguards relating to health privacy. Members of the public and research participants value privacy highly, and inability to ensure it could affect participation. Canadian common law and legislation require a full and comprehensive disclosure of risks during informed consent, including anything a reasonable person in the participant or patient's position would want to know. Research ethics policies require similar disclosures, as well as full descriptions of privacy related risks and mitigation strategies at the time of consent. In addition, the right to withdraw from research gives rise to a need for ongoing consent, and material information about changes in privacy risk must be disclosed. Given the research ethics concept of "non-identifiability" is increasingly questionable, policies based around it may be rendered untenable. Indeed, the potential inability to ensure anonymity could have significant ramifications for the research enterprise.

Keywords
privacy, confidentiality, informed consent, health information, biobanking, identifiability, research ethics, health law

Introduction

More and more people have biological samples and health information stored with a range of public and private entities, including direct-to-consumer health and ancestry genetic testing companies, clinical laboratories, cohort initiatives and large-scale biobanks. Personal health information includes many types of information, ranging from qualitative or demographic information to genomic data and even biobanked tissue itself (1). And with the rise of Big Data research initiatives, personal information from a range of sources is being compiled, shared and analyzed in ever more complex ways (2). Often, individuals are asked to provide consent for the storage and use of their information for research and other permitted purposes. In other circumstances, policies allow research to be conducted without consent.

The obligation to maintain the privacy of the research participant is foundational to biomedical research. It is mentioned in virtually every research ethics guideline, including well-established international statements (3,4), national policies (5,6), and professional ethics codes (7,8). Privacy is expected by the general public and research participants, and it is a key component of public trust in the research enterprise (9). But there is growing concern about the challenges of keeping participant information private and confidential (10,11). Growth in sophisticated information technologies that can facilitate data breaches along with increasing collection and sharing of digitized health information may make it more difficult for researchers, public research institutions and private companies to maintain this obligation (12).

When consent is required for research involving health information and biological samples, the relevant consent process often includes information about data protection, the entities and individuals that will have access, and why confidentiality cannot always be guaranteed. But given the shifting information technology landscape, to what degree does the consent process need to evolve, if at all, to reflect emerging privacy and data protection concerns? Have privacy risks – and the public concerns

ISSN 2561-4665

and perceptions about those risks – changed enough to warrant re-consenting for samples that were collected with data protection guarantees that are no longer realistic? What privacy risks ought to be disclosed to participants and when? And are the promises of anonymity that are so often made to research participants and research ethics boards still tenable?

In this article we explore these questions through the lens of Canadian health law and research ethics policies. The goal is to map the nature of the emerging consent challenges. As research involving health information and biological samples becomes increasingly common, essential and complex, the issues associated with privacy will intensify. Here, we seek to highlight several areas that warrant immediate attention.

The Emerging Privacy Challenge

A number of recent studies have highlighted how emerging computational strategies can be used to identify individuals in health data repositories managed by public or private institutions (13). And this is true even if the information has been anonymized and scrubbed of all identifiers (14). A study by Na et al., for example, found that an algorithm could be used to re-identify 85.6% of adults and 69.8% of children in a physical activity cohort study, "despite data aggregation and removal of protected health information" (15). A 2018 study concluded that data collected by ancestry companies could be used to identify approximately 60% of Americans of European ancestry and that, in the near future, the percentage is likely to increase substantially (16). Such concerns have led at least one company to offer "anonymous" genome sequencing (17). Furthermore, a 2019 study successfully used a "linkage attack framework" – that is, an algorithm aimed at re-identifying anonymous health information – that can link online health data to real world people and thus, as suggested by the authors, clearly demonstrates "the vulnerability of existing online health data"(18). And these are just a few examples of the developing approaches that have raised questions about the security of health information framed as being confidential. Indeed, it has been suggested that today's "techniques of re-identification effectively nullify scrubbing and compromise privacy" (19).

In addition, data breaches involving health information are on the rise. A study from the US found that the rate of data breaches increased by 70% between 2010 and 2017 (20,21). Sensitive demographic and financial information is commonly compromised (22). In Canada, there have been a number of high profile breaches involving publicly held health information (23,24). In British Columbia, for example, a 2016 incident led to a province-wide freeze of biomedical research involving health information (25). Data breaches in the private sector are also increasing, with most being caused by malicious or criminal attacks (26,27). In addition, there are examples of inappropriate sharing of data for research purposes, as exemplified by the potential class action lawsuit in the United States that accuses the University of Chicago of sharing identifiable patient data with Google (28).

There have also been highly publicized instances of genetic repositories being used by law enforcement agencies for the purpose of criminal investigations. Probably the most famous was when genetic information from a direct-to-consumer genealogy company was used to uncover the identity of and apprehend the Golden State murderer (29,30). Since then, there have been numerous other examples of repositories of genetic samples being used in similar situations (31). While the use of genetic databases in this context does not necessarily implicate health research biobanks and cohort studies, it once again emphasizes how information that was collected under a presumption of confidentiality may be used in controversial and unexpected ways. These cases have also made the privacy issues very public – as highlighted by this New York Times headline: "Sooner or Later Your Cousin's DNA Is Going to Solve a Murder … The price may be everyone's genetic privacy" (32). This coverage may impact public perceptions and concerns about privacy issues and, perhaps, expectations regarding what is disclosed during the consent process.

The emergence of powerful technologies and re-identification strategies coupled with a rising number of privacy controversies has prompted some commentators to go so far as to suggest that the entire concept of privacy and anonymity is dead (27,33,34). Indeed, it has been suggested that we now live in the era of privacy nihilism – a time when it is becoming near impossible to maintain privacy and to control what others can learn about you (35). Of course, not all data repositories are the same and the risk of a data breach likely differs significantly depending on many factors. Still, these privacy controversies and technology trends highlight that we may need to reconceptualise how we think about and frame privacy for the purposes of consent. This seems particularly so given that much of consent law is based on what a research participant may want to know about risks and not necessarily merely those that are most significant.

Privacy and Public Perceptions

The public, and patients in particular, are mostly supportive of the idea of sharing their health information and biological material for research purposes (36,37). However, that support is often contingent on the promise of privacy and the de-identification of information (38), a strategy that, as noted, may not be effective at protecting privacy. Despite the technological reality that it has become near impossible to guarantee its existence, people still care about privacy, particularly in the context of biological samples (39) and health information (37). A 2017 study from the US found that "[n]inety percent of participants agreed health information privacy was important to them; 64% agreed that they worried about the privacy of their health information" (37). A 2019 study from Canada found that while most people support the contribution of personal data for research purposes, "respondents placed high importance on deidentification of data" and only "58% were confident about the privacy and security procedures in place" (40).

This work highlights the degree to which support for research is linked to assurances of privacy (38). These concerns may be heightened in the context of genetic information. While the way in which individuals think about privacy in the context of health information can vary considerably (41), genetic information is generally viewed, rightly or not (42), as being especially sensitive. Studies have consistently found that, if asked, people will say they are concerned about both genetic privacy (43,44) and data breaches in relation to online data (45).

We need to take care not to oversimplify privacy concerns. Individual circumstances will, for example, change how people rate privacy as a concern in the context of research. A patient or an individual with a sick family member may view the privacy concerns of health information differently than a person who is not directly or indirectly involved in a research initiative (46), and there is also variation within these groups (47). Likewise, whether a research participant is paid or unpaid for their involvement may also change the calculus (44). People balance risks differently for many reasons. Still, the body of available research suggests people are concerned about privacy and the potential for data breaches (38).

Studies have also found that the public is concerned about data custodians sharing personal information without consent. A 2018 survey, for example, found that 85% of Americans are concerned that DTC genetic testing companies will share genetic data without permission and 71% are worried medical researchers will do the same (48). This concern about privacy can impact willingness to use online services (49) and to participate in research that involves the collection of health information and genetic material, such as biobanking (50). Such data again demonstrates public attention to privacy in this context and the need to be sensitive to these issues during the consent process.

Privacy issues are also getting more and more media coverage (32,51,52), which may then increase concern for privacy by making people more aware of the relevant issues. Research has shown that media coverage of a risk can make that risk seem more likely. This is due to the “availability bias”, a well-known cognitive bias that affects our perceptions (53). And there are indications that an increasing percentage of the public wish to retain significant control over their health information. Indeed, we have seen the rise of the concept of “biorights” (54) – that is, the desire for research participants to control and profit from biological material donated for research purposes. This movement has been stirred, at least in part, by both the perception that biological samples are worth a significant amount of money and controversies associated with the mishandling of biological samples (55), such as the much publicized case of Henrietta Lacks (39).

These kinds of developments may heighten the public’s interest in and concern about privacy issues, which may, in turn, trigger interest in heightened disclosure in the context of consent. Indeed, a 2018 survey from the US found that “data privacy” was ranked as the single biggest concern in relation to the private sector, above job creation, access to healthcare and education (56). A 2016 study by the Office of the Privacy Commissioner of Canada found that the public is becoming increasingly concerned about protection of personal privacy, with 92% saying they are at least somewhat concerned (57). Thirty-seven percent say they are extremely concerned, which is up from 25% in 2012 (57).

Consent, Re-consent and Reporting

The collection and use of biological samples and digitized health information for research purposes has long generated legal and research ethics issues (55,58). It seems likely that the privacy issues outlined above may further complicate these challenges. Here we focus more narrowly on two specific and practical questions: what privacy risks need to be disclosed and when recontact and reconsent is required. Again, our aim is to map these challenges to inform future conceptual and empirical work.

Required Disclosure

In the clinical setting, all material information must be disclosed as part of the consent process. The courts have generally treated disclosure expansively to include anything that a reasonable person in the patient’s position would want to know (59). And this obligation is even more onerous in the context of medical research (60,61). Generally, informed consent for medical research requires “full and frank disclosure” of all relevant facts, probabilities and opinions a reasonable person might be expected to consider before giving consent, even if minor disclosures might cause unnecessary worry (60). Canadian consent statutes similarly specify categories that suggest a full and comprehensive disclosure of risks (62).

While the technical risk of a harmful data breach may remain low, the risk is real and, given what we know about how people view privacy concerns in this context, information about this risk may be material. Indeed, what is deemed to be material information about risk in the eyes of the law does not necessarily have to correspond to a scientifically or statistically substantial risk (63). Rather, the question is more whether a reasonable person, who would likely be aware of dominant social and media discourses about health information privacy concerns, would want related information about privacy risks disclosed. Professional guidelines support the idea that even information about “statistically remote” risks must be disclosed if they are “of a serious nature” (64). As such, the changing nature of the privacy threats seems likely to warrant a more robust delineation of privacy risk during informed consent.

The *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* [TCPS2] remains the most important research ethics policy in Canada, as all federally funded research must adhere to it via research ethics board (REB) oversight

(5). For informed consent, the TCPS2 requires patients be provided with "a plain language description of all reasonably foreseeable risks and potential benefits" (5), as well as:

> an indication of what information will be collected about participants and for what purposes; an indication of who will have access to information collected about the identity of participants; a description of how confidentiality will be protected; a description of the anticipated uses of data; and information indicating who may have a duty to disclose information collected, and to whom such disclosures could be made (5).

Other sections of the TCPS2 expand on disclosure requirements related to privacy and confidentiality. Notably, researchers must "describe measures for meeting confidentiality obligations and explain any reasonably foreseeable disclosure requirements" both in application materials submitted to research ethics boards and "during the consent process with prospective participants" (4). REBs, in assessing proposed measures to achieve data security, must consider risks to participants "should the security of the data be breached, including risks of re-identification of individuals" (5). These provisions, taken together, suggest a requirement to disclose known and *potential* privacy risks, including risks to data security. Disclosure of potential risks, in our view, should encompass what we presently know about how participant data can be compromised, such as studies that show that re-identification of anonymized data is possible (14,15,18,19).

One issue arising from these standards is that a more robust disclosure of privacy risks may cause individuals to be less likely to agree to participate in biobank and cohort studies. Research has found that people generally rate specific privacy concerns as seeming more severe than abstract concerns (65). In other words, the more detailed the disclosure, the more potential participants view participation as problematic. Researchers may thus be concerned about scaring patients away from participation (66). Yet, from a legal perspective, this concern is not a valid justification for nondisclosure. Indeed, if the disclosure of a risk impacts willingness to participate, it is exactly the kind of information that must generally be disclosed. In addition, international research ethics norms stress that the rights of the research participants are paramount. As stated in the Declaration of Helsinki: "While the primary purpose of medical research is to generate new knowledge, this goal can never take precedence over the rights and interests of individual research subjects." (67) Besides, negative reactions to full disclosure may have more to do with a lack of understanding of the technicalities surrounding data security than with the need to be fully informed and, as such, may be countered or addressed by a robust disclosure process that educates participants about data security.

Ongoing Consent and Reconsent

Research consent in Canada and internationally often involves the participant agreeing to secondary use of de-identified information and/or biological materials for future research that is undetermined at the time of consent (5,68,69). In a system using this type of research consent, when is recontact and reconsent required?

The TCPS2 requires that privacy measures be maintained for the entire life cycle of health information, including "collection, use, dissemination, retention and/or disposal." (5) In general, any change or development to relevant risks that is material to the participant's decision to participate or continue to have his/her information stored will trigger a legal obligation to recontact (59). This is in keeping with the previously noted law concerning disclosure for informed consent (59,60,61). The risk need not be material in an evidentiary sense, but merely in a subjective sense, in that the participant would find it relevant to ongoing participation (63,70). Given evidence that participants care about privacy (46,49), any material change in privacy and confidentiality risk would likely warrant recontact. This raises the issue of whether and when technological developments in re-identification strategies that reduce the effectiveness of existing privacy safeguards could trigger a need for recontact and reconsent. Again, given existing law and public perception data, a compelling argument could be made that they would if they put the relevant database at an increased risk of a breach.

In the context of research ethics, a longstanding principle of international and Canadian policies is the right to withdraw from participation in research at any time (3,4,5). While there are a few exceptions to this right – such as quarantining in the context of some infectious disease research (71) – this is a near universally accepted research ethics norm that aligns with the conceptualization of informed consent as an ongoing process (5). In order for ongoing consent to continue to be informed, the TCPS2 requires participants be "given, in a timely manner throughout the course of the research project, information that is relevant to their decision to continue or withdraw from participation" (5). As noted, it is possible under the TCPS2 to provide a broad consent for future secondary use of identifiable information (5). But this does not vitiate the right to withdraw at any time or the requirement to provide information that may be material to a decision to continue participation.

Given that non-identifiability may no longer be a reality for tissues and some types of information, perhaps the biggest challenge lies with the concept of "non-identifiable" information and its application in the TCPS2. Article 5.5B states that researchers are not required to seek participant consent for research that "relies exclusively on the secondary use of non-identifiable information" (5). Moreover, Article 2.4 of the TCPS currently allows for secondary research use of "anonymous" information or biological materials without REB review, as long as "the process of data linkage or recording or dissemination of results does not generate identifiable information" (5). This policy may be increasingly controversial as re-identification techniques improve and spread (14,15). Indeed, the evolution of re-identification technologies and strategies, while still far from representing a broadly applicable threat, may compel a reconsideration of these kind of exceptions to consent and ethics review.

People care deeply about privacy, including not only actual participants but also and especially the parents of minor participants (48,50). It seems likely that re-consenting could lead to withdrawals and that may make research difficult and affect the integrity of data (72). However, research ethics policies are designed to protect participants. More importantly, the law of disclosure does not change in the face of competing researchers' interests (3,4,5). Privacy-related information may cause some participants to withdraw from research. But, rightly or not, there are no legal and ethical norms that would suggest disclosure practices can be modified for the purpose of avoiding withdrawals or refusals to consent.

Finally, there seems little doubt that data breaches and any unauthorized access to or disclosure of identifiable or re-identifiable participant information must be disclosed. Questions remain as to how we can define the moving target of "re-identifiability" and its relationship to risk of participant harm, but erring on the side of always notifying participants of a breach would be prudent. There is a clear duty pursuant to legislation in most Canadian jurisdictions to inform participants affected by privacy breaches (73). This duty requires, on the one hand, a strengthening of existing research ethics policies, such as by clearly emphasizing participants' rights to be re-contacted and re-consented where a material threat to data privacy emerges, and, on the other hand, a reconsideration of ethical requirements, such as less emphasis on data anonymization and de-identification as mitigation for data security risks.

Conclusion

In this age of Big Data research, it seems likely that there will be an increasing need to collect biological samples and digital health information. At the same time, as computational and information technologies progress, the risks to privacy will expand. The same technologies that are making health information more clinically and scientifically valuable – such as inexpensive sequencing, online databases and AI – are the tools that can also be leveraged to compromise privacy.

The promise of anonymity is becoming ever more tenuous. Yet, it remains a foundational component of the research ethics policies that underlay and enable health research. The potential inability to ensure anonymity could have significant ramifications. The public values privacy and, as a result, the inability to ensure it could re-frame the consent process and how participants think about participation in research initiatives. It would be valuable to generate more data on the public's and research participants' tolerance for the risk of privacy breaches and to engage in research to help determine how best to communicate those risks in a balanced manner.

The fact that privacy is highly valued affirms and even heightens the legal obligation to disclose privacy related risks. Material information about risks, including risks associated with privacy, must be disclosed. If there is a material change in risk, this information needs to be disclosed and may trigger an obligation to reconsent. Given the rapid rate of development in AI and other domains relevant to data protection, important questions arise as to what kind of advances in reidentification technologies could constitute a material change in risk. Such considerations will require ongoing monitoring by the research ethics community and seem likely, at the very least, to complicate the way we think about the protection of privacy.

Remerciements
Les auteurs remercient Robyn Hyde Lay pour ses commentaires et suggestions constructifs. Ce travail a été financé par les projets de Génome Canada *Childhood Asthma and the Microbiome—Precision Health for Life: The Canadian Healthy Infant Longitudinal Development (CHILD) Study* et *Precision Medicine CanPREVENT AMR: Applying Precision Medicine Technologies in Canada to Prevent Antibody Mediated Rejection and Premature Kidney Transplant Loss*. Les organismes subventionnaires qui ont soutenu cette recherche sont notamment : les Instituts de recherche en santé du Canada (numéros de subvention RES0041866 et RES0038357) et Genome Alberta (numéros de subvention RES0040987 et RES0041085).

Acknowledgements
The authors thank Robyn Hyde Lay for her helpful comments and suggestions. This work was funded by the Genome Canada projects *Childhood Asthma and the Microbiome—Precision Health for Life: The Canadian Healthy Infant Longitudinal Development (CHILD) Study* and *Precision Medicine CanPREVENT AMR: Applying Precision Medicine Technologies in Canada to Prevent Antibody Mediated Rejection and Premature Kidney Transplant Loss.* Specific funders that supported this research include: the Canadian Institutes of Health Research (grant numbers RES0041866 and RES0038357), and Genome Alberta (grant numbers RES0040987 and RES0041085).

Conflits d'intérêts
Aucun à déclarer

Conflicts of Interest
None to declare

Responsabilités des évaluateurs externes
Les recommandations des évaluateurs externes sont prises en considération de façon sérieuse par les éditeurs et les auteurs dans la préparation des manuscrits pour publication. Toutefois, être nommé comme évaluateurs n'indique pas nécessairement l'approbation de ce manuscrit. Les éditeurs de la *Revue canadienne de bioéthique* assument la responsabilité entière de l'acceptation finale et de la publication d'un article.

Peer-reviewer responsibilities
Reviewer evaluations are given serious consideration by the editors and authors in the preparation of manuscripts for publication. Nonetheless, being named as a reviewer does not necessarily denote approval of a manuscript; the editors of *Canadian Journal of Bioethics* take full responsibility for final acceptance and publication of an article.

Édition/Editors: Patrick Gogognon & Aliya Affdal
Évaluation/Peer-Review: Michelle Mello & Mackenzie Graham

Affiliations
1 Health Law Institute, Faculty of Law, University of Alberta, Edmonton, Alberta, Canada

Correspondance / Correspondence: Timothy Caulfield, caulfield@ualberta.ca

Reçu/Received: 1 Nov 2019 **Publié/Published:** 20 Jul 2020

Les éditeurs suivent les recommandations et les procédures décrites dans le Code of Conduct and Best Practice Guidelines for Journal Editors de COPE. Plus précisément, ils travaillent pour s'assurer des plus hautes normes éthiques de la publication, y compris l'identification et la gestion des conflits d'intérêts (pour les éditeurs et pour les auteurs), la juste évaluation des manuscrits et la publication de manuscrits qui répondent aux normes d'excellence de la revue.

The editors follow the recommendations and procedures outlined in the COPE Code of Conduct and Best Practice Guidelines for Journal Editors. Specifically, the editors will work to ensure the highest ethical standards of publication, including: the identification and management of conflicts of interest (for editors and for authors), the fair evaluation of manuscripts, and the publication of manuscripts that meet the journal's standards of excellence.

References

1. Ogbogu U, Burningham S, Caulfield T. The right to control and access genetic research information: does McInerney offer a way out of the consent/withdrawal conundrum. UBCL Rev. 2014;47:275.
2. Powles J, Hodson H. Google DeepMind and healthcare in an age of algorithms. Health and technology. 2017;7(4):351-67.
3. Council for International Organizations of Medical Sciences, World Health Organization. International Ethical Guidelines for Health-related Research Involving Humans. 2016. [Accessed 2019 Sep 5].
4. World Medical Association. WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects. 2018 Jul 9. [Accessed 2019 Sep 5].
5. CIHR, NSERC, SSHRC. Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS2 (2018). 2017 Oct 12. [Accessed 2019 Sep 4].
6. United States Government. Electronic Code of Federal Regulations: 690.111 Criteria for IRB approval of research. [Accessed 2019 Sep 5].
7. Canadian Medical Association. CMA Code of Ethics and Professionalism. 2018 Dec. [Accessed 2019 Sep 5].
8. American Medical Association. Code of Medical Ethics: Privacy, confidentiality & medical records. [Accessed 2019 Sep 5].
9. Serenko N, Fan L. Patients' perceptions of privacy and their outcomes in healthcare. International Journal of Behavioural and Healthcare Research. 2013;4(2):101-22.
10. Kolata G. Your data were 'anonymized'? these scientists can still identify you. New York Times. 2019 Jul 23. [Accessed 2019 Aug 30].
11. McCoy TH, Hughes MC. Preserving patient confidentiality as data grow: implications of the ability to reidentify physical activity data. JAMA network open. 2018;1(8):e186029-.
12. Dankar FK, Ptitsyn A, Dankar SK. The development of large-scale de-identified biomedical databases in the age of genomics-principles and challenges. Hum Genomics. 2018;12(1):19.
13. Hayden EC. Privacy loophole found in genetic databases. Nature News. 2013 Jan 17. [Accessed 2019 Oct 4].
14. Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. Identifying personal genomes by surname inference. Science. 2013;339(6117):321-4.
15. Na L, Yang C, Lo CC, Zhao F, Fukuoka Y, Aswani A. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. JAMA network open. 2018;1(8):e186040-.
16. Erlich Y, Shor T, Pe'er I, Carmi S. Identity inference of genomic data using long-range familial searches. Science. 2018;362(6415):690-4.
17. Begley S. Amid privacy concerns, startup becomes first consumer DNA company to offer anonymous sequencing. STAT. 2019 Sep 19. [Accessed 2019 Oct 2].
18. Ji S, Gu Q, Weng H, Liu Q, Zhou P, He Q, Beyah R, Wang T. De-Health: all your online health information are belong to us. arXiv preprint:1902.00717. 2019 Feb 2.
19. Lubarsky B. Re-identification of "anonymized data". UCLA L. REV. 1701;1754(2010).
20. McCoy TH Jr, PerlisRH. Temporal trends and characteristics of reportable health data breaches, 2010-2017. JAMA. 2018;320(12):1282-1284.
21. HIPAA. Study reveals 70% increase in healthcare data breaches between 2010 and 2017. HIPAA Journal. 2018 Sep 28. [Accessed 2019 Aug 30].
22. Jiang JX, Bai G. Types of information compromised in breaches of protected health information. Annals of Internal Medicine. 2019 Sep 24.
23. Gerein K. Former AHS worker inappropriately accessed 1,300 health records, viewed thousands more. Edmonton Journal. 2016 Sep 26. [Accessed 2019 Aug 30].
24. CBC News. AHS warns 7,000 patients their personal health information compromised in email hack. 2019 Aug 22. [Accessed 2019 Aug 30].
25. Hunter J. Privacy breach in B.C. health ministry led to freeze on medical research data. The Globe and Mail. 2016 Apr 26. [Accessed 2019 Aug 30].
26. Solomon H. Cost of Canadian data breaches continues to rise, says study. IT World Canada. 2018 Jul 11. [Accessed 2019 Aug 30].
27. Burt A, Geer D. The end of privacy. New York Times. 2017 Oct 5. [Accessed 2019 Aug 30].

28. Robbins R. Potential class action lawsuit accuses the University of Chicago of sharing identifiable patient data with Google. Stat News. 2019 Jun 26. [Accessed 2019 Aug 30].
29. The Associated Press. DNA from genealogy site used to catch suspected Golden State Killer. CBC News. 2018 Apr 26. [Accessed 2019 Aug 30].
30. Kaiser J. We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans. Science. 2018 Oct 11. [Accessed 2019 Sep 4].
31. Marcus AD. Customers handed over their DNA. the company let the FBI take a look. The Wall Street Journal. 2019 Aug 22. [Accessed 2019 Aug 30].
32. Murphy H. Sooner or later your cousin's DNA is going to solve a murder. New York Times. 2019 Apr 25. [Accessed 2019 Aug 30].
33. Lufkin B. The reason you can't be anonymous. BBC. 2017 May 29. [Accessed 2019 Aug 30].
34. Keshavan M. 'There's no such thing as anonymity': With consumer DNA tests, sperm banks reconsider long-held promises to donors. STAT. 2019 Sep 11. [Accessed 2019 Sep 11].
35. Bogost I. Welcome to the age of privacy nihilism. The Atlantic. 2018 Aug 23. [Accessed 2019 Aug 30].
36. Kim J, Kim H, Bell E, Bath T, Paul P, Pham A, Jiang X, Zheng K, Ohno-Machado L. Patient perspectives about decisions to share medical data and biospecimens for research. JAMA network open. 2019;2(8):e199550-..
37. Sanderson SC, Brothers KB, Mercaldo ND, Clayton EW, Antommaria AH, Aufox SA, Brilliant MH, Campos D, Carrell DS, Connolly J, Conway P. Public attitudes toward consent and data sharing in biobank research: a large multi-site experimental survey in the US. American Journal of Human Genetics. 2017;100(3):414-27.
38. Jones KH, Daniels H, Squires E, Ford DV. Public views on models for accessing genomic and health data for research: mixed methods study. Journal of Medical Internet Research. 2019;21(8):e14384.
39. Dasgupta I, Bollinger J, Mathews DJ, Neumann NM, Rattani A, Sugarman J. Patients' attitudes toward the donation of biological materials for the derivation of induced pluripotent stem cells. Cell Stem Cell. 2014;14(1):9-12.
40. McCormick N, Hamilton CB, Koehn CL, English K, Stordy A, Li LC. Canadians' views on the use of routinely collected data in health research: a patient-oriented cross-sectional survey. CMAJ open. 2019;7(2):E203.
41. Haeusermann T, Fadda M, Blasimme A, Tzovaras BG, Vayena E. Genes wide open: Data sharing and the social gradient of genomic privacy. AJOB Empirical Bioethics. 2018;9(4):207-21.
42. Evans JP, Burke W. Genetic exceptionalism. Too much of a good thing? Genetics in Medicine. 2008;10(7):500.
43. Clayton EW, Halverson CM, Sathe NA, Malin BA (2018) A systematic literature review of individuals' perspectives on privacy and genetic information in the United States. PLoS ONE 13(10):e0204417.
44. Kaufman DJ, Murphy-Bollinger J, Scott J, Hudson KL. Public opinion about the importance of privacy in biobank research. American Journal of Human Genetics. 2009;85(5):643-54.
45. Canadian Marketing Association. Data privacy study: what the canadian consumer really thinks. 2018 May 24. [Accessed 2019 Aug 30].
46. Chen A. Treating 'genetic privacy' like it's just one thing keeps us from understanding people's concerns. The Verge. 2018 Oct 31. [Accessed 2019 Aug 30].
47. Siminoff LA, Wilson-Genderson M, Mosavel M, Barker L, Trgina J, Traino HM. Confidentiality in biobanking research: A comparison of donor and nondonor families' understanding of risks. Genetic Testing and Molecular Biomarkers. 2017;21(3):171-7.
48. NORC. Genetic testing: ancestry interest, but privacy concerns. NORC Center for Public Affairs Research. 2018 Jul. [Accessed 2019 Aug 30].
49. Baruh L, Secinti E, Cemalcilar Z. Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication. 2017;67(1):26-53.
50. Antommaria AH, Brothers KB, Myers JA, Feygin YB, Aufox SA, Brilliant MH, Conway P, Fullerton SM, Garrison NA, Horowitz CR, Jarvik GP. Parents' attitudes toward consent and data sharing in biobanks: A multisite experimental survey. AJOB Empirical Bioethics. 2018;9(3):128-42.
51. Mervosh S. Jerry Westrom threw away a napkin last month. it was used to charge him in a 1993 murder. New York Times. 2019 Feb 17. [Accessed 2019 Aug 30].
52. Mroz J. A mother learns the identity of her child's grandmother. a sperm bank threatens to sue. New York Times. 2019 Feb 16. [Accessed 2019 Aug 30].
53. Tversky A, Kahneman D. Judgment under uncertainty: Heuristics and biases. Science. 1974;185(4157):1124-31..
54. Hayden MA. The burgeoning biorights movement: its legal basis, what's at stake, and how to respond. BCL Rev.. 2018;59:1775.
55. Caulfield T, Murdoch B. Genes, cells, and biobanks: Yes, there's still a consent problem. PLoS Biology. 2017;15(7):e2002654.
56. Brown D. Americans are more concerned with data privacy than job creation, study shows. USA Today. 2018 Nov 9. [Accessed 2019 Aug 30].
57. Office of the Privacy Commissioner of Canada. 2016 Survey of Canadians on Privacy. 2016 Dec. [Accessed 2019 Aug 30].
58. Vayena E, Blasimme A. Health research with big data: Time for systemic oversight. Journal of Law, Medicine & Ethics. 2018;46(1):119-29.
59. Reibl v. Hughes, [1980] 2 SCR 880, 1980 CanLII 23 (SCC).
60. Halushka v. University of Saskatchewan (1965) 53 DLR (2D) 436.
61. Robertson G, Picard E. Legal Liability of Doctors and Hospitals in Canada, 5th Edition. Toronto, Canada: Carswell/Thomson Reuters, 2017.

62. Nelson E, Ogbogu U. Law for Healthcare Providers. Toronto: LexisNexis, 2018;88-89.
63. Nelson E. Informed consent: reasonableness, risk, and disclosure. In: Downie J, Gibson E. (eds.) Health Law at the Supreme Court of Canada. Toronto, Canada: Irwin Law Inc: 2007. p.145-168.
64. Evans KG. Consent: A guide for Canadian physicians. CMPA. Updated 2016 Jun. [Accessed 2019 Aug 30].
65. Gerber N, Reinheimer B, Volkamer M. Investigating people's privacy risk perception. Proceedings on Privacy Enhancing Technologies. 2019;2019(3):267-88.
66. Couper MP, Singer E, Conrad FG, Groves RM. Risk of disclosure, perceptions of risk, and concerns about privacy and confidentiality as factors in survey participation. Journal of Official Statistics. 2008;24(2):255.
67. World Medical Association. Declaration of Helsinki: Ethical Principals for Medical Research Involving Human Subjects. 2013.
68. Master Z, Nelson E, Murdoch B, Caulfield T. Biobanks, consent and claims of consensus. Nature Methods. 2012;9(9):885.
69. Allen C, Joly Y, Moreno PG. Data sharing, biobanks and informed consent: a research paradox. McGill JL & Health. 2013;7:85.
70. Arndt v. Smith, [1997] 2 SCR 539, 1997 CanLII 360 (SCC).
71. Murdoch B, Caulfield T. The challenge of human challenge research models: A Canadian perspective. Medical Law International. 2017;17(4):273-84.
72. Junghans C, Jones M. Consent bias in research: how to avoid it. Heart. 2007;93(9):1024.
73. CMPA. The new reality of reporting a privacy breach. 2018 Nov. [Accessed 2019 Sep 4].