BLOCKCHAIN™ IN HEALTHCARE TODAY

Open Data: Implications on Privacy in Healthcare Research

David Chen

Affiliations: Schulich School of Medicine & Dentistry, University of Western Ontario, London, Canada

Corresponding Author: David Chen, Schulich School of Medicine & Dentistry, University of Western Ontario, London, Canada. dchen362@uwo.ca

Keywords: Open Data, Data Management, Blockchain, Healthcare Research

Section: Review

The advent of open data in health care has increased healthcare innovation, with the publication of complete datasets aggregated by private and public entities that lead to efficiency through crowdsourcing working code, facilitating research into personalized medicine, and publishing reproducible data pipelines for experimental validation.

However, there lacks an internationally recognized definition for health data governance at the scope of individual health data and open source big data, which bring about a discussion about the implications of open data on data privacy. First, healthcare data sourced directly from public healthcare systems: by whom and for what purpose is these data used for within the context of healthcare research. Second, health data from private research: the regulations needed for mutual disclosure. Third, personal user-generated health data: safeguards in a digital era needed to prevent misappropriation and abuse.

This paper addresses the opportunities of open data in healthcare research in a digital age without transparent regulation. The consequence of open data on privacy leads to a framework of four safeguards for stakeholders: public education, operational transparency, regulation for accountability, and validation of research ethics. It also pioneers public policy direction for a balanced agenda between privacy and healthcare research.

INTRODUCTION

Open data are defined by the Government of Canada as structured data, that is machine-readable, freely shared, used, and built on without restrictions.[1] The development of structured crowdsourcing, data donation, and participatory surveillance leverages public sector datasets to be used for robust secondary healthcare research at significantly lower costs compared to primary clinical research approaches.[2] Open data host such as Github (known for its open source community projects, and repository such as Open Government, a data collection aggregated by the Government of Canada) also contribute to the significant potential in developing knowledge of diseases, improving validity, and utility of medical diagnostics and treatment options.

From an economical standpoint, open data stand to create a value proposition upwards of $300 billion across the world.[3] The origin of this value stems from its role to enable innovation in disease diagnosis,[4] monitoring and treatment,[5] maintaining the cost effectiveness of treatment,[6] and innovating new healthcare approaches and products to improve quality of care.[7] To wholly capture the value of open data in health care, this requires a robust standard for data governance and right to usage that takes into account the need for individual privacy, government regulation, and changes to make the data as versatile and effectively used as possible.[8]

Healthcare data host sensitive information that is protected due to the proprietor's right to privacy.[9] Raw data collected from primary studies can be revised with anonymized identifiers in place of sensitive identifiers, so that the participant's right to privacy is respected.[9] There also exists pressure in favor of open data used in healthcare research and to promote transparency in healthcare operations.[10] This raises further discussion on the balance needed when individuals have ownership of their health data: the ability to make informed decisions when sharing or keeping these health data confidential and the extent to which this autonomous discretion is defined and used in practice.

ROLE OF GOVERNMENT REGULATION OF PUBLIC- AND PRIVATE-SOURCED DATA

Government has the legislative power to form policies and set an overall tone by which the private sector and individual users use and share open data. Government public health agencies should set defined rules on data governance, release, with a particular focus on privacy, accountability, confidentiality, and proprietary rights that are based on the value proposition of open data rather than how easily shared the data should be.[11] Leaders in government can direct the responsibility of open data across multiple public healthcare agencies for the purpose of transparency through open data releases on accessible platforms. This direction of responsibility can extend internationally; for example, Canada overseas as co-chair of the open government partnership (OGP), a multilateral initiative that aims to promote government transparency and large-scale open government and public data reforms in partnership with the private sector.[12] The OGP is the first step toward large-scale open data in an internationally collaborative forum. The United Kingdom leads by example by ranking first in international indexes for open data implementation, stemming from its commitment to quarterly updates on progress in self-implementation and high impact of initiatives at scale.[13] This commitment engages subnational governments to work harmoniously with national approaches in piloting a federated search service for open data.

Government regulation also has the power to directly influence legal and economic to maximize the value proposition of open data usage, while still addressing the legitimate needs of privacy from major stakeholders and rights to proprietorship for individuals and organizations. Taking a lesson from Estonia, who is a leader in digital solutions in public administration ecosystems and electronic banking, these policies should include definitions on access, usage, and protocols needed to notify data proprietors, and an institutional focus on centralized digital architectures for storage and data transfer.[14] It is the role of government officials to uphold standards while adapting policies for data accessibility and versatility among theirs use cases. In spite of this heed to caution, the government should also promote private sector companies to address public health data shortages by collecting and releasing data with effective protections. At a municipal level, education in robust analytical skills when manipulating open data provides significant potential for new innovation in a constantly evolving field of healthcare research.[15]

STANDARD OF INDIVIDUAL PRIVACY

The concept of open data involves a social network of people, policies by which governance is defined, cultural practices and behaviors, and the state of technology infrastructure over time. The dynamics of this open data ecosystem is ever changing as new fields and datasets are introduced or remodeled. This is particularly important when non-healthcare data are integrated with healthcare data, leading to new interdisciplinary consequences such as unethical research and breaches in privacy safeguards.[16]

It is understood that the nature of health details sensitive and identifying information by which discussion with trained health professionals is kept confidential. The data used in administrative and primary treatment approach at the healthcare facility while attending a patient is expected to be upheld to the highest standard of professional to patient confidentiality.[17] Further down the line, secondary use of patient data in translational research instigates a new divide between privacy and open data. Even with few pseudonymized data points, modern data processing and statistical inferences can predict missing data points and even identify individuals at an unprecedented level from public and private repositories. This poses a paradox in open data policy: the more detailed a dataset, the more valuable it becomes for innovation, and the more likely sensitive personal data can be traced back to individuals through alternative and often unethical means.[18] There needs to be a balance between the value and sensitivity of open datasets, erring on the side of caution for privacy until holistic usage policies have been put into place.

The landmark Canadian case, McInerney v. MacDonald (1992), established that patients have the right to access information of their own records despite physicians owning the physical record.[19] The court found that healthcare providers hold patient information in trust on behalf of the patient, who retains their right to access these data. However, ambiguity remains: the Supreme Court found that right to access can be denied by the provider if there exists a significant likelihood of an adverse effect due to such information on the medical record. The resolution concludes that the owner of the physical record is responsible for controlling access in accordance to privacy law. When frameworks lack clarity between definitions of open, closed, and shared data, this undermines civilian trust.

Case Study: COVID-19 Crisis Research

Within the context of a pandemic crisis such as the SARS-CoV-2 virus, the speed of accessing data and conducting research toward a vaccine directly impacts the progress made. Due to the fast-paced demand for crisis research, the need for open data in health care becomes crucial in concerted international efforts, where thousands of teams across a multitude of private and public sectors collaborate in parallel. New inventions and innovations abound in an environment that rewards speed of development to product timelines. For example, complete genomic sequences sourced from individual patient data are updated to GenBank repositories and are made open source in good faith,[20] where a range of researchers to high school students at hackathons propose new ways to tackle this pandemic.

This pits the value of open data in health care, its open source, inexpensive approach, with its greatest concern: privacy. Crisis research questions stakeholders in public and private sectors how we plan on addressing the quick release of healthcare data with a minimum standard in the robustness of privacy protection.[21] It also brings the question on what data should be shared publicly; in this case, should the genomic data of individuals affected by SARS-CoV-2 found in GenBank be shared with public or private researchers if it is in the best interest of society at large? More data often lead to refined healthcare models and treatment approaches that account for more unique factors.

It remains unclear at what stage the consent is given, as well as if the consent can be retracted, then at what speed will personalized data be removed following the retraction of consent. This means that if consent can be revoked by the civilian, the speed of reaction by GenBank to respond remains unclear and allows for anyone to continue to use these data until they are effectively removed. As a safeguard, the rapid use of genomic data for treatment research should yield to patients who withhold these highly sensitive personal data from an open platform.

Case Study: Intelligent Interfaces in Health Care

Deloitte has conducted a 2019 review of technology in health care, where they identified several fields of innovation that will have a significant impact within the next 5 years.[22] In particular, the review noted a marked increase in the degree of cooperation between healthcare providers and private sector technology industries for digital experience, cybersecurity, and intelligent interfaces.[22] The innovative technologies include IBM Watson, an artificial intelligence capable of answering questions posed in natural language,[23] and Google's DeepMind Health, used to serve patients, nurses, and doctors as mobile medical assistants.[24] These systems encompass fields of genomics, drug discovery, and patient monitoring.

The DeepMind Health Streams application allows healthcare practitioners to be notified of changes to patient's vital signs and deliver real time information to mobile devices.[24] In developing and rural countries, this allows healthcare practitioners to improve their effective standard of care despite barriers in equipment and distance from major centers. The use of personal health data to facilitate patient monitoring and research is mutually contractual, with proprietary technology owned by the private sector and healthcare data collected by public healthcare systems.[24] Google's Project Nightingale achieves this objective: it has partnered with the largest nonprofit healthcare system in the USA, Ascension, in a project aimed to predict emergent health data.[25] The ethical issue of data governance and usage when the technology and health care integrate into one entity becomes difficult to quantify. Secure solutions in cybersecurity and protection of privacy rights when conducting experimental research with patient clinical data are essential in gaining civilian trust in a personalized field of medicine.

Case Study: Care.data—Undermining Trust

The sale of personal health data to commercial entities has become a very sensational media topic that often reports on misappropriation of data and failure of full disclosure between consenting parties, which lead to ambiguity in data governance. Care.data was a public research repository hosted by the Health and Social Care Information Centre (HSCIC, now NHS Digital) that extracted data from general surgeries into a centralized database.[26] English citizens who participated in general practitioner (GP) surgeries reported in this database were informed that these personal health data would be uploaded to HSCIC unless express objection was obtained by informing their GP.[26] Data were anonymized to prevent identification, and identifiable data could only be contained through legal due process.[26]

Care.data was reputable as a research resource for exploratory data analysis, monitoring of specific treatment outcomes, and progress in personalized medicine approaches. The controversy arose when the data were also made available to numerous private sector companies such as the pharmaceutical industry and insurance companies, which have vested interests in sensitive information on patients for economic gain. In 2014, as part of an organization audit, it was determined that pseudonymous and identifiable data were sold for financial gain to organizations despite the supposed open data framework that suggested privacy protection.[27] Following a request for Freedom of Information, the HSCIC made a statement that suggested the identity of individuals may be ascertained through Care.data in combination with other data sources.[28]

This case study sheds light on the minimal degree of anonymization of Care.data and the limited use case of pseudo anonymity in a modern era of Internet of Things. Algorithmic technologies within the last 10 years have been developed, which can massively harvest and analyze data to predict identifiable information from piecewise data with high accuracy. Therefore, the degree of pseudonymity that is effective is inversely proportional to the improvements in classification algorithms to a point where even the most robust efforts to anonymize data artificially while still maintaining theirs usability no longer protects data privacy.[29] By this account, access to sensitive public health open data must be monitored on a case-by-case basis, and the implications of emerging technologies should be consulted as new developments arise. The lesson of this issue is not meant to instigate paranoia; it is a heed to caution about sharing potentially sensitive data without mutual disclosure and the threats to security that exist from vested interests in the private sector.

LIMITATIONS OF THE PRIVACY PARADOX

Health information systems face the looming conundrum often coined as the Privacy Paradox. The paradox is based on the inconsistencies between people's privacy attitudes and their associated behavior.[30] For complex systems to operative effectively in the healthcare space, an equilibrium must be adaptively maintained between the usage of individual's information and protecting privacy. Yet the demand for both quality healthcare services and privacy of personal information can simultaneously be met if appropriately addressed. The architecture of privacy regulation lends itself to regulation at each step of the personal data economy: collection, storage, usage, and information transfer. Solove addressed the need for regulation in his suggestion of contractual agreements between parties during data transfer, adding control points throughout the data economy that makes certain transfers bounded by regulation.[31] Thereby, the Privacy Paradox implicates that regulation of privacy exceeds self-management at the individual level but requires restructuring of governance and revision of contractual agreements between individuals and third parties.

The most clear-cut approach to contractual agreements between parties in the data economy involves explicit consent intended to honor the autonomous right for self-governance of personal data.[31] However, the synergistic interplays of the data economy do not easily distill into the binary nature of consent, and even if it could, the constant need for approval of consent can inundate individuals with requests beyond practical means. Furthermore, explicit consent may not wholly succeed in this endeavor, given that usage and value of individual data are unpredictable. The need to reengineer legacy systems with modern approaches to individual data management is a monumental challenge and will require extensive testing and implementations of novel technologies that translate into actionable and measurable outcomes within the healthcare data privacy space.

BLOCKCHAIN: AN EMERGENT TECHNOLOGY FOR INFORMATION SYSTEMS

Blockchain is an emergent technology that decentralizes data across multiparty systems that transact and access information simultaneously. Distributed applications based on blockchain involve information that interfaces across multiple nodes of the network, conveying a sense of transparency while continuing to regulate data management through smart contracts that can execute automated approval of individual consent.[32] Stakeholders clearly understand who has access to their data, who has used their data, when they were used, and in what manner, all of which remain a gray area in the current health data economy infrastructure.[33] The nature of blockchain as a distributed ledger technology and its inherent immutability ensures the integrity of data and prevents alterations after they have been appended to the network. Blockchain also employs cryptographic hashes of appended blocks of data, which encrypts messages during transit to protect sensitive information of patients until they reach the intended target, where the data are decrypted with legitimate permissions. The European General Data Protection Regulation (GDPR) prohibits the usage of sensitive personal data unless express consent is achieved, such as through blockchain-integrated smart contracts. The combination of these intrinsic blockchain features safeguards against data loss compared to conventional systems reliant on singular, centralized authorities and paves the way for a GDPR-compliant healthcare information system.

Ransomware attacks have also critically revealed the prevailing security flaws of healthcare facilities with maladaptive data practices that lend itself to systemic exploitation.[34] Investments into more secure systems now can outweigh the initial costs over time. Finally, the oversight of pseudonymity of healthcare records in the face of advanced predictive analytics and big data makes it difficult to truly anonymize data intended for research purposes. Also, the case of Care.data has shown how easily conventional data management practices can be compromised and how quickly public trust in other parties using their personal data can be lost. Blockchain technology maximizes security of information storage and mediates accessibility when sharing healthcare data records, which can be useful in applications beyond primary healthcare venues, such as clinical trials and monitoring systems for out-of-hospital care.[35]

A limitation of the blockchain implementation lies in the need to reengineer legacy systems and its cost per transaction as part of the blockchain system which can total a sizable cost. The implementation of a blockchain system would replace entire electronic databases, medical records, and registries, as well as prevent costly data breeches in order to maximize cost-efficiency over time.[33] Blockchain poses a novel architecture for modern healthcare data management in its approach to patient-centered care with security first and should be noted as an emergent technology within the digital health space.

RESPONSIBLE DEVELOPMENT OF OPEN DATA

Engagement between the public and commercial private sector is necessary for delivering effective outcomes in healthcare research to a standard of personal privacy. Neither risk-averse nor high-risk authorities should wholly dictate the spectrum of open data policy; instead, civilians should challenge both sides on each side to engage in establishing an agenda that benefits both healthcare research efforts and respects privacy standards. Existing platforms in the United States have shown substantial improvement toward the provision of open data for health research. However, a sustained effort is needed to improve associated metadata and hyperlinks, so that researchers will use these data and consider those as a valuable, trustworthy source.[36]

First, public engagement should include scaled awareness campaigns that focus on the full disclosure: benefits and risks of sharing personal health data should factor in empirical evidence while promoting the potential use cases for innovation. This will produce an ongoing dialogue between policy makers; authorities in the private sector and civilians meant to increase civilian trust in government policy and understanding the use for open data in research initiatives that can lead to public good. The difficulties of public engagement focus on how the media may continue to portray sensational news on the shortcomings of open data in favor of supplementing its constructive dialogue.[37]

Second, transparency in who will be using the personal health data and for what purpose according to the core regulation processes outlined in the Open Data Principles will be required. Transparency needs regulation and enforcement of such regulation. Full disclosure and a notification platform to inform individuals of their use of healthcare data should be included in the proposed regulations. The practical implementation of these regulations may differ in format.

Third, a shift in the mass-scale regulation of data usage by commercial industry should be proposed. With big data, users can regain control of their own data from businesses and should be able to make an informed decision on who they decide to share their data with and at what cost to either party. In this model, the default proprietor of healthcare data lies with the individual rather than businesses or the government. One of the main problems lies in the need for existing business models to rapidly adapt, particularly due to the increasing degree of partnership between private sector researchers and governments.

Fourth, major stakeholders need to be educated with the modern computing skill and research ethics needed to take advantage of open healthcare data. Through a deeper understanding of the source of healthcare open data and its implications, can the privacy needs be wholly appreciated? Standards must be set by industry authorities, researchers, and medical professionals to communicate the duality of open data within the context of privacy in an increasingly shared online world. Furthermore, education can empower civilians at a local scale to advocate for privacy rights to address community needs through grassroots initiatives.

CONCLUSION

The open data movement has presented potential in fostering innovation and increasing operational transparency. Open data have reduced costs of advancing healthcare research and contributed to the improvement of healthcare provision by sharing information in a connected world. The issue of data privacy requires novel approaches to simultaneously meet the research needs while actively engaging public trust through open data integration that preserves individual privacy. Policymakers need to establish shared regulatory frameworks among proprietors and regulatoryauthorities, which meet an equilibrium between privacy safeguards, prevent commercial exploitation, and keep consenting parties informed of their personal data. It is the responsibility of research authorities to advocate with key policymakers and guide the process of outlining a revised multi-stakeholder agenda. Open data have the potential to save millions of lives when used in research appropriately. However, the most significant advantage of sharing health data still instigates debate. More work must be done regarding its greatest flaw: privacy.

Funding Statement

Author certifies that this article received no funding in any part by a supporting organization.

Conflict of Interest

Author certifies there is no conflict of interests in this article.

Contributors

None.

References

1. Open Data 101. 2019 [cited 17 April 2020]. Available from: https://open.canada.ca/en/open-data-principles
2. Chignard S. A brief history of open data—Paris innovation review. Parisinnovationreview.com; 2020 [cited 16 April 2020]. Available from: http://parisinnovationreview.com/articles-en/a-brief-history-of-open-data
3. Manyika J, Chui M, Farrell D, Van Kuiken S, Groves P, Doshi E. Open data: Unlocking innovation and performance with liquid information. *McKinsey Digital*. 2020 [cited 19 April 2020]. Available from: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information#
4. Alizadehsani R, Roshanzamir M, Abdar M, et al. A database for using machine learning and data mining techniques for coronary artery disease diagnosis. *Scientif Data*. 2019;6(1):1–13.
5. Oliveira R, Cherubini M, Oliver N. MoviPill. Proceedings of the 12th ACM International Conference on Ubiquitous Computing. 2010 [cited 10 April 2020];251–260. Available from: https://dl.acm.org/doi/abs/10.1145/1864349.1864371
6. Mejia J, Mejia A, Pestilli F. Open data on industry payments to healthcare providers reveal potential hidden costs to the public. *Nat Commun*. 2019 [cited 20 April 2020];10(1). Available from: https://doi.org/10.1038/s41467-019-12317-z
7. Greene W. Can open data drive innovative healthcare? *Forbes*. 2020 [cited 16 April 2020]. Available from: https://www.forbes.com/sites/techonomy/2015/10/01/can-open-data-drive-innovative-healthcare/#2795ca617f28
8. Priisalu J, Ottis R. Personal control of privacy and data: Estonian experience. *Health Technol*. 2017;7(4):441–451.
9. Amis R. Developing a research data policy. Learn-rdm.eu; 2020 [cited 21 April 2020]. Available from: http://learn-rdm.eu/wp-content/uploads/red_LEARN_Elements_of_the_Content_of_a_RDM_Policy.pdf

10. Kostkova P. A roadmap to integrated digital public health surveillance. Proceedings of the 22nd International Conference on World Wide Web. ACM Digital Library; 2020 [cited 24 April 2020]. Available from: https://dl.acm.org/doi/abs/10.1145/2487788.2488024
11. Cowan D. Perspectives on open data: Issues and opportunities. Canadian Index Wellbeing; 2020 [cited 22 April 2020]. Available from: https://uwaterloo.ca/canadian-index-wellbeing/sites/ca.canadian-index-wellbeing/files/uploads/files/perspective_on_open_data-issues_and_opportunities.pdf
12. Robert M. Canada action plan 2018. Open Government Partnership; 2020 [cited 25 April 2020]. Available from: https://www.opengovpartnership.org/wp-content/uploads/2019/01/Canada_Action-Plan_2018-2020_EN.pdf
13. Global Report. The Open Data Barometer; 2020 [cited 22 August 2020]. Available from: https://opendatabarometer.org/4thedition/report/#findings_recommendations
14. Kassen M. Open data politics in Estonia: Advancing open government in the context of ubiquitous digital state. *SpringerBriefs Polit Sci*. 2019;37–67.
15. Coughlan T. The use of open data as a material for learning. *Educ Technol Res Dev*. 2019;68(1):383–411.
16. Verhulst S, Noveck B, Caplan R, Brown K, Paz C. The open data era in health and social care. Gov Lab; 2014 [cited 23 April 2020]. Available from: https://www.thegovlab.org/static/files/publications/nhs-full-report.pdf
17. Bailey T. Duty of confidentiality. The Royal College of Physicians and Surgeons of Canada; 2016 [cited 21 April 2020]. Available from: http://www.royalcollege.ca/rcsite/bioethics/cases/section-3/duty-confidentiality-e
18. Triggle N. Care.data: How did it go so wrong? BBC News; 2014 [cited 24 April 2020]. Available from: https://www.bbc.com/news/health-26259101
19. Forest G, L'Heureux-Dube C, Gonthier C, Stevenson W, Iacobucci F. McInerney v. MacDonald—SCC cases (Lexum). Supreme Court Judgements; 2012 [cited 27 April 2020]. Available from: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/884/index.do
20. NCBI SARS-CoV-2 resources. National Library of Medicine; 2020 [cited 24 April 2020]. Available from: https://www.ncbi.nlm.nih.gov/genbank/sars-cov-2-seqs/
21. Stauffacher D, Hattotuwa S, Weekes B. The potential and challenges of open data for crisis information management and aid efficiency. ICT4Peace Foundation; 2012 [cited 24 April 2020]. Available from: https://ict4peace.org/wp-content/uploads/2012/03/The-potential-and-challenges-of-open-data-for-crisis-information-management-and-aid-efficiency.pdf
22. Wong N, Pagsanjan A, Peeler R, Chavan S. Tech trends 2019 health care perspective. Deloitte; 2019 [cited 19 April 2020]. Available from: https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/sante-et-sciences-de-la-vie/deloitte_healthcare-perspective-2019.pdf
23. Knight W. IBM's Watson is everywhere—But what is it? MIT Technology Review; 2016 [cited 27 October 2020]. Available from: https://www.technologyreview.com/2016/10/27/156388/ibms-watson-is-everywhere-but-what-is-it/
24. Lomas N. TechCrunch; 2019 [cited 25 April 2020]. Available from: https://techcrunch.com/2019/09/19/google-completes-controversial-takeover-of-deepmind-health/
25. Marks M. Everyone is asking the wrong question about Google's new health care project. Slate Magazine; 2020 [cited 22 April 2020]. Available from: https://slate.com/technology/2019/11/google-ascension-project-nightingale-emergent-medical-data.html

26. Vezyridis P, Timmons S. Understanding the care.data conundrum: New information flows for economic growth. *Big Data Soc*. 2017;4(1):205395171668849.
27. Cooper C. 40 per cent of GPs plan to opt out of the NHS big data sweep, due to a lack of confidence in the project. The Independent; 2014 [cited 19 April 2020]. Available from: https://www.independent.co.uk/life-style/health-and-families/health-news/40-per-cent-of-gps-plan-to-opt-out-of-the-nhs-big-data-sweep-due-to-a-lack-of-confidence-in-the-9083806.html
28. Bhatia N. Register of approved data releases—A freedom of information request to NHS Digital. WhatDoTheyKnow; 2014 [cited 20 April 2020]. Available from: https://www.whatdotheyknow.com/request/register_of_approved_data_release
29. Nagel E, Frith J. View of anonymity, pseudonymity, and the agency of online identity: Examining the social practices of r/Gonewild | First Monday. First Monday; 2015 [cited 23 April 2020]. Available from: https://firstmonday.org/article/view/5615/4346
30. Li X, Motiwalla L. Unveiling consumers' privacy paradox behaviour in an economic exchange. *Int J Bus Inform Syst*. 2016;23(3):307.
31. Solove D. The myth of the privacy paradox. *George Washington Univ Law School*. 2020;89(10).
32. Dagher G, Mohler J, Milojkovic M, Marella P. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain Cities Soc*. 2018;39:283–297.
33. Chen H, Jarrell J, Carpenter K, Cohen D, Huang X. Blockchain in healthcare: A patient-centered model. *Biomed J Sci Tech Res*. 2019;20(3).
34. Slayton T. Ransomware: The virus attacking the healthcare industry. *J Legal Med*. 2018;38(2):287–311.
35. Vazirani A, O'Donoghue O, Brindley D, Meinert E. Implementing blockchains for efficient health care: Systematic review. *J Med Int Res*. 2019;21(2):e12439.
36. Martin E, Law J, Ran W, Helbig N, Birkhead G. Evaluating the quality and usability of open data for public health research. *J Public Health Manag Pract*. 2017;23(4):e5–e13.
37. Bourgault J. How the global open data movement is transforming journalism. WIRED; 2020 [cited 24 April 2020]. Available from: https://www.wired.com/insights/2013/05/how-the-global-open-data-movement-is-transforming-journalism/