Managing Health Information Privacy During the COVID-19 Pandemic: Considerations and Perspectives from Around the Globe

Given the extraordinary circumstances of the COVID-19 pandemic, the importance of managing the privacy of health information, and applying governance principles, has been heightened. This case study explores the challenges of managing privacy during this pandemic, particularly since new technologies are being used to control disease spread and mitigate the impact to personal and economic consequences.

Background:

Following the public health emergency decree on January 30th, the World Health Organization (WHO) declared COVID-19 a pandemic on March 11, 2020[1]. The rapid spread of the disease, along with global transmission, prompted this pandemic declaration. The impact of the disease and measures to try to control the spread have created profound health and economic consequences, with some stating that a global recession is underway[2].

Privacy of information was discussed by Organization for Economic Cooperation and Development (OECD)[3] in their April 2020 article outlining considerations being explored and temporary changes that are being implemented to existing privacy regulations. Included in these discussions are trade-offs in privacy management to stop disease spread and temporary changes in privacy regulations. As OECD stated, "few countries have frameworks in place to support the extraordinary contact-tracing and population-wide surveillance measures envisaged" in fighting COVID-19. The data era in which we live affords new opportunities to address disease spread, yet data governance, and regulations already in place in various countries around the world, require we be transparent in managing the COVID-19 data. Thus, tantamount to the extraordinary measures being deployed is the need to be transparent about changes, and stoppage of these changes when the pandemic has cleared.

Health data privacy practices regarding COVID-19 data have varied considerably. They are constantly changing as data sharing challenges arise, best practices are identified, new technology is used in treatment, vaccine trials are

advanced, and contact tracing expands. The Global Privacy Assembly, a privacy organization of global privacy and data protection regulators has created a special member page[4] with the most up to date privacy information about how countries are managing the privacy of COVID-19 data. Privacy International[5] has also published information and guidance on global health privacy.

Problem Discussion:

Data Sources and Privacy Protection

The pandemic has highlighted many uses of health data. To ensure a proper understanding of the data collected, an understanding of where the data comes from is essential. Typically, data sources are defined as primary or secondary. Primary sources are the patient health record, vital statistics, or censuses. New primary sources of data brought about by the pandemic are, for example, those created by businesses when screening employees or visitors, or data derived from contact tracing. Secondary sources are those created from primary sources, such as indexes or registries[6].

Regardless of the source of data or the intended use, privacy of the individual whom the data represents is dependent upon how the data is collected, stored, and exchanged. The intended use of the data, regulatory requirements, and the privacy expectations of the individuals require measures to protect the data from being tied to the individual. De-identification, the removal of identifiers from the data, may satisfy privacy requirements in some countries, such as the United States (US) under the Health Insurance Portability and Accountability Act (HIPAA). However, the European Union (EU) under the General Data Protection Regulations (GDPR) requires anonymization, which goes a step further than de-identification by removing all linkages between the identifiers and the data[7,8].

Collection, Access, and Disclosure of Health Information

Collection of health information by healthcare organizations and providers must be authorized by legislation. An individual's consent alone does not authorize organizations or public bodies to collect an individual's health information. In this time of public health crisis, we need to continue to respect an individual's right to privacy.

Individuals continue to access their own information for a variety of reasons, including continuing healthcare. While organizations may be challenged to respond to requests in previously accepted reasonable time frames, they must continue to respond.

Similarly, health information may be disclosed on a limited as-needed basis when there is a risk of significant harm to the health or safety of the public. Healthcare organizations must document their decisions to disclose – or not disclose – health information in response to requests for health information.

Secondary Use of Data, Big Data

In the context of curtailing the COVID-19 pandemic, countries have created databases of millions of peoples' sensitive personal information while potentially overlooking privacy concerns. Government and non-government agencies are relying on this sensitive personal information for various secondary uses such as research, vaccine and medicine development, business analytics, insurance claim processing, and a multitude of population health management activities. Many prominent health organizations such as National Institutes of Health (NIH[9]), European Centre for Disease Prevention and Control (ECDC)[10], WHO and several private organizations provide open access to select COVID-19 secondary data and statistics for the research purpose.

Big data, as evidenced by the massive COVID-19 databases, is key in the management and forecasting of COVID-19. Enormous epidemiological and scientific data sets are being utilized by the health authorities and scientific community to make more informed decisions in fighting the coronavirus and preventing similar pandemics in the future[11]. The sensitive personal information on screening, testing, contact tracing, clinical management, and mortality is sometimes outsourced to private parties which raises privacy and data management concerns. The integrating of additional sources of data from social media, geolocation information, and proximity data (e.g., apps on a mobile phone), further compounds the potential privacy issues of the COVID-19 databases.

Massive administration of vaccines, the next phase of COVID-19 management, may witness large-scale collection of sensitive personal information. Many aspects of future life — employment, higher studies, travel, attending a conference, hospital visits, and so forth, may depend on

> Massive administration of vaccines, the next phase of COVID-19 management, may witness large-scale collection of sensitive personal information.

an individual's vaccination data. This data, which may be available in numerous platforms, may be accessed and shared between various agencies across the world. The implications of data tracking as part of mass surveillance activities may also raise privacy concern.

Maintaining privacy and confidentiality of sensitive personal information post-COVID-19 must be a priority area for all kinds of organizations. The absence of strong data protection laws in a majority of countries, and across borders, as discussed in the whitepaper, **Privacy of Health Information, an IFHIMA Global Perspective**, will make this challenging.

Balancing Individual Privacy with Community Benefit

The pandemic has required rapid responses to information sharing requests, particularly in contact tracing of potentially affected persons[12]. Reactionary responses to situations have, at times, resulted in privacy breaches. One example is the use of older, unsecure technology to transmit messages by a pager system, resulting in an easily hacked information system[13].

Privacy legislation would normally inhibit the release of identifiable information to researchers. In a state of emergency such as COVID-19, broader powers may be enabled in terms of a looser data anonymization process. Thus epidemiologists, researchers and data scientists are granted broader access to support faster and better research outcomes[14].

Privacy Concerns Associated with COVID-19 Testing

A specific area of privacy concern is related to COVID-19 testing. News programs, social media and websites have reported on many issues related to testing. These include the lack of available testing sites[15], delays in implementing testing and receiving results[16], and the long lines[17] where individuals are either standing in the elements or sitting in their cars lined up for blocks on end. We have undoubtedly seen in this reporting images of healthcare workers in full PPE, swabbing the nose of an individual with the individual's face visible or car license plate, or family members in plain view[18].

Not only are hospitals offering drive-through or walk-up COVID-19 testing sites, pharmacy chains, shopping centers, and lab providers are offering these services as well[19]. Other places of employment, such as meatpacking plants, have also implemented testing[20].

With this rapid growth of testing, privacy concerns increase.

- How is privacy afforded during testing?
- Is the technology used to collect and transmit the individual's health data secure, and is it being sent to the correct location?
- How is the media prevented from recording and broadcasting recognizable images of those undergoing the tests?
- Are the employees who staff the test sites trained on patient privacy?

> Each state , provincial, health authority, or country's privacy laws must be referenced for guidance to ensure compliance with privacy laws and garner trust by the individuals and the public at large .

Test providers must address these questions to ensure the privacy of each individual presenting for testing. Each state , provincial, health authority, or country's privacy laws must be referenced for guidance to ensure compliance with privacy laws and garner trust by the individuals and the public at large.

Privacy Concerns Associated with Contact Tracing

To slow or eliminate the spread of COVID-19, health departments in countries around the world have rapidly employed the use of contact tracing[21]. This involves identifying individuals who have been in contact with an individual with COVID-19, informing them of their potential exposure, and referring them for testing[22].

This modern-day pandemic has introduced the technology of digital contact tracing apps, made to assist with mitigating the spread of the virus. The apps use GPS technology to track and record an individual's movements. The app "pings" anonymous identifier data between users of the app who come near one another and serves as a notification system[23].

Some developers of this technology, i.e. Google and Apple, have pledged to disable the system after the pandemic and have stated they do not have access to identifying information. Although use of the apps in the U.S.A. and Europe has been low, there is still a concern over future access to information[24]. Privacy concerns, along with perceptions regarding individual freedoms, might be hampering the widespread use of these apps. In the USA, the app developers are not considered covered entities under HIPAA, and therefore are not bound by HIPAA.

As with any electronic health data collected, stored, transmitted and shared, there are concerns with data from contact tracing being truly anonymized. There is the potential for third-party access or use, data use beyond what was the originally intended, and of course, breaches[25].

Automating COVID-19 contact tracing is desirable in the face of the overwhelming scope of the pandemic. However, the collection of personal information, including location data using mobile phone technology, is an enormous responsibility with enormous risk for misuse and unauthorized secondary data use for other purposes.

The principles of privacy should apply to apps, including collecting the least amount of information necessary and allowing individuals to control how their personal information is collected and used. Individuals should have the opportunity to consent to activate the contact tracing app. People diagnosed with COVID-19 should also be allowed to decide whether to disclose to public health officials the contact log stored on their phones[26].

Human oversight of technology and mitigation of risk is necessary to protect these privacy principles.

As with any electronic health data collected, stored, transmitted, and shared, there are concerns with data from contact tracing being truly anonymized, the potential for third-party access or use, use of data beyond the originally intended use, and of course, breaches.

Risk assessments of contact tracing apps also need to include a plan to decommission the data collected and strong access and disclosure policies. (See the discussion of Records Processing Standards and Health Information Exchanges in the above-mentioned whitepaper.)

Privacy Impact Assessments (PIA)

The response to COVID-19 had decidedly changed business processes in both the short term and the foreseeable future.

As discussed in the whitepaper, **Privacy of Health Information, an IFHIMA Global Perspective,** when we collect health information, we are tasked with the responsibility to avoid risks, harm, and breaches of privacy. Change in business process should automatically trigger an assessment and documentation of health information privacy and security risks and mitigation strategies.

In the early days of the COVID-19 response, public health and emergency measures often overrode previously routine business models and healthcare delivery. While healthcare providers and organizations were expected to continue to make the best privacy-protecting decisions possible, regulators acknowledged the need to quickly respond to public interest needs with less strenuous documentation of risk assessments, mitigation plans, and agreements. This does not allow for negligence or malicious collection or misuse or breach of health information. A PIA should explore these potential issues.

Remote Working

Many organizations expedited the remote working of some of their workforce or mobilized their workforce to work in new temporary locations, such as in mobile testing sites and care units. Now, organizations should review these workforce changes to identify privacy and security risks and implement mitigation strategies, including business-grade hardware and software deployment, secure networking, data storage and transfer, and auditing to monitor appropriate access to health information. Security risk assessments are useful tools to conduct a comprehensive assessment of risks and identify mitigation strategies.

Privacy impact assessments are appropriate tools to assess the privacy risks of health information using new business models and technology like contact tracing apps. The Alberta OIPC has published its review of the Privacy Impact Assessment submitted by the Alberta Health Services[27]. This review, as an example, is useful to organizations to conduct their own PIA.

Similar COVID-19 screening data collection (whether in paper or digital format) by non-health service employers and businesses can be guided by the discussion of privacy risks and mitigation strategies.

Vendors should also undertake a PIA to identify the impact of their personal information handling practices, and implement strategies to manage, minimize or eliminate these risks[28].

(See the discussion Information Sharing and Information Management Agreements in the **whitepaper**.)

Telehealth

One of the benefits of the pandemic experience is the explosion of telehealth adoption by healthcare providers across the world. In large part, this is due to the increased reimbursement and funding from insurance providers and governments and the need to physically deliver care outside the normal care settings.

Care providers need to complete a risk assessment before selecting and implementing a telehealth solution and provide additional privacy and security awareness training for healthcare providers, staff, and patients. See the discussion on privacy awareness training in the **whitepaper**.

In the rapid response to the pandemic, many healthcare providers used a variety of unsecure public video conferencing and messaging solutions to transmit confidential health information. Many of these platforms were not designed for this use and resulted in unanticipated risks. Now, we expect healthcare providers to carefully review technology options and implementation and select vendors who adopt a privacy by design approach and build in privacy-friendly default settings in their telehealth solutions. Select these default settings to:

- Strengthen access controls
- Clearly announce new callers
- Mute users' video/audio feeds on entry
- Allow business users to seek other users' consent
- Minimize the collection of personal information or data[29].

Conclusion

It is important to remember that we are currently in disaster mode. Regardless of the type of disaster, e.g., hurricanes, cyclones, terrorist attacks, health organizations can become overwhelmed by the demand for services while changing priorities and care delivery models. The additional demand tests the capability of the health service to effectively manage health information[30]. This 'command and control' situation has left health organizations and services scrambling to adjust and balance the need to control this disease with the protection of information.

> Sound governance principles must be applied, especially in this new frontier.

Sound governance principles must be applied, especially in this new frontier. IFHIMA discussed these in our **information governance whitepaper.** HIM roles in protecting privacy, advocating for patients, and guiding providers on health information collection, maintenance, use, and disclosure are increasingly necessary now, and will not diminish once the pandemic subsides.

Call to Action

As emergency measures end, we will return to 'normal' privacy practices for collection, use, and disclosure of personal information. However, as a result of the pandemic, newly created or heightened areas of health information management may require HIM professionals to:

1. Collaborate with healthcare leaders and business owners to ensure that appropriately executed information management, business associate, and information sharing agreements are in place. These agreement must enable information to flow during normal operations, as well as a pandemic or disaster.
2. Effect secure destruction of pandemic-related records at the end of reasonable retention periods. For example, pre-screening done by business owners and employers, including healthcare organizations, should be destroyed as per information governance procedures.
3. Pro-actively review and update records management practices. These must address telehealth, remote monitoring, synchronous live virtual care encounters (i.e., telephone consultations, video conference), asynchronous virtual care encounters (i.e., exchange of messages and information via patient portals, secure email messaging, or blood glucose monitoring devices), and mobile health or m-health, (i.e., transmitting data via blue-tooth enabled devices).

An Australian Viewpoint of Privacy in a Pandemic-The Effect on the Psyche of the Australian Population

In Australia in late 2019 we experienced some of the worst bushfires that we have ever seen in our country. This resulted in a heightened level of anxiety and worry in the public psyche, which has then been further compounded over the uncertainty surrounding the COVID-19 and an unknown future[31].

Patients with a serious mental illness in Australia are at a greater risk of having increased mental health challenges during a pandemic, particularly with the implementation of measures such as social distancing that can put this population at a very high risk of suicide and unhealthy behaviours. The stigma of mental illness pervades across certain cultures such as the Indigenous Australian population and any potential privacy exposure can also result in an unwillingness to participate in treatment[32].

Mental health issues are further exacerbated when patients also have to deal with extended periods of time in quarantine[33]. The recent lockdown of social housing apartments in Melbourne[34] presented some critical concerns about privacy breaches because the apartments are usually overcrowded and provide very little privacy for such treatment as a telehealth consultation. Alternative methods such as web and text messaging services may be a better option to ensure absolute privacy[35].

Further thought must be given by health services in Australia into the way in which mental health clients in the community receive care during this pandemic to ensure that privacy is maintained at a high-level[36].

Privacy Impact Assessments[37] for the health service are usually carried out to review the privacy protection standards of the health service. However, consideration should also be given to the development of a Privacy Impact Assessment for the client before proceeding with the service delivery.

COVID-19 Pandemic and Data Privacy: Current Scenario in India

India is travailing through COVID-19 pandemic with the second-highest number of cases globally, as of this writing. During this pandemic, one of the most debated topics among the public was data privacy. It became a new norm for millions of people to mandatorily or voluntarily provide their personal information to government agencies for the purpose of screening and contact tracing. The handling of data privacy during the current pandemic scenario in India can be observed in two contexts, i.e. smart phone enabled COVID monitoring apps and management of health information of COVID positive cases.

India is one among the few countries to come out with a smart phone enabled app called 'Aarogya Setu' to combat the pandemic. This app was developed to manage contact tracing, create awareness and issue safety warnings to the public. Despite the voluntary nature of this app, all government and many private organizations made it mandatory for its staff to install this app on their smartphones. As of now more than 110 million people have installed `Aarogya Setu'[38] despite privacy concerns raised by experts and citizens. No major privacy breaches have been officially reported.

All data related to COVID positive cases are collected and processed through a centralized mechanism under the control of Indian Council of Medical Research (ICMR) and such data cannot be used for research purpose without ICMR approval.

In spite of strict conditions privacy breaches have occurred when local level bodies identified COVID affected persons through the use of a sticker on a home or place under quarantine. Examples of breaches have included photos of the property and affected persons being uploaded to social media.

India needs strong regulations for ensuring data privacy and security similar to GDPR and HIPAA. Our health system and regulators should also give importance to the concerns of people related to data privacy issues during pandemics.

USA – HIPAA Applications and Enforcement During a Pandemic

The overarching federal health information privacy laws in the United States are the Health Insurance Portability and Accountability Act's (HIPAA) privacy and security rules. As with any law, misinterpretations abound, especially during a national health crisis, such as the COVID-19 pandemic experienced in 2020.

The Department of Health and Human Services Office for Civil Rights (OCR), the enforcement agency for HIPAA, has provided periodic privacy guidance in response to the changing healthcare modalities and needs of the American public that resulted from the pandemic.

A bulletin[39] posted on the OCR website reminded covered entities under HIPAA that the privacy rule already provided the ability to share protected health information (PHI) during emergencies. It also reinforced the provision that if in the healthcare provider's judgment, it was in the best interest to share PHI with a patient's family, friends, or others involved in the patient's care and for notification, it was permissible to do so.

Another major point of this bulletin was to notify covered entities (CEs) implementing a limited waiver of HIPAA sanctions and penalties during the pandemic. Understanding the imposition of challenges faced by providers dealing with a rapidly escalating population of patients, the agency sought to allay fears of sanctions when, despite best efforts and without malice, certain HIPAA violations might occur.

Subsequent bulletins provided privacy guidance on telehealth, first responders, business associates, community-based testing sites, news media access and restrictions, and contacting former COVID-19 patient about blood donation opportunities[40].

Telehealth providers were informed of acceptable platforms over which to provide remote communication with patients[41]. "Public-facing" products such as TikTok and Facebook Live are explicitly prohibited as they do not provide for private interaction between the patient and provider. "Non-public facing" products are permissible, as they provide for privacy and typically employ end-to-end encryption of the data being transmitted.

Privacy guidance to community-based testing sites included using secure technology to gather and transmit patient information, establishing "buffer zones" to prevent the media or others from observing or recording individuals being

testing, and controlling foot and car traffic to provide distance to decrease the ability of others to overhear information[42]. Guidance on media coverage explained that providers must obtain a valid HIPAA authorization from each patient whose PHI may be accessible to the media before granting access[43]. Simply obscuring or masking patients' identities after recording but before broadcasting does not meet the HIPAA standards.

OCR is suspending the rule that prohibits Business Associates from sharing PHI with public health authorities upon request if it is not permitted in the business associate agreement[44]. This rule suspension provides for quicker exchange of COVID-19 data to public health authorities.

Of note, there has been no guidance as of the writing of this paper regarding contact tracing. Privacy concerns in this area, discussed herein, should be considered when training the individuals who are involved in contact tracing.

IFHIMA Authors

Sharon Campbell
Lecturer, Health Information Management/Project Officer
Curtin University/Midwest Mental Health & Community Alcohol and Drugs
BSc,HIM. MHlthAdmin
Sharon is a HIMAA board director and chairs their Privacy and Security Special Interest Group
https://www.linkedin.com/in/sharon-campbell-242537135/

Jean L. Eaton
BA Admin (Healthcare), CHIM
Practical Privacy Coach with Information Managers Ltd. which provides privacy, health information and practice management consultation services to healthcare providers throughout Canada.
https://www.linkedin.com/in/Jeaneaton

Lorraine Fernandes
RHIA serves as IFHIMA President (2019-2022) and Board Liaison to IFHIMA Privacy Workgroup. Lorraine is Principal at Fernandes Healthcare Insights, a data governance focused practice.
https://wwwlinkedin.com/in/lorraine-fernandes-07723b1/

Dr. Sabu Karakka Mandapam
M.App.Sc, PhD
A Professor of Health Information Management and an Associate Dean, Manipal College of Health Professions, Manipal Academy of Higher Education, Manipal, India and also serves as a member in AHIMA International Advisory Council.
https://www.linkedin.com/in/km-sabu-6259a012/

Dorinda M. Sattler
MJ, RHIA, CHPS, CPHRM is a Clinical Assistant Professor of HIM at Indiana University Northwest. Dorinda is also the Consultant/Owner of Sattler Healthcare Consulting, Inc. which provides HIM and Risk Management Consulting services to healthcare providers, malpractice attorneys, and insurers throughout the state of Indiana.
https://wwwlinkedin.com/in/dorinda-sattler-45414a92

About IFHIMA

The International Federation of Health Information Management Associations (IFHIMA) is a non-governmental organization (NGO) in official relations with the World Health Organization (WHO). The Federation, founded in 1968, acts as the global voice of the health information management profession to support delivery of healthcare services and activities and to share best practices. IFHIMA is committed to the advancement of health information management practices and the development of its members for the purpose of improving health data and health outcomes.

Learn more about IFHIMA on LinkedIn.

References

1. https://pubmed.ncbi.nlm.nih.gov/32191675/
2. https://www.worldbank.org/en/news/press-release/2020/06/08/covid-19-to-plunge-global-economy-into-worst-recession-since-world-war-ii
3. http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/
4. https://globalprivacyassembly.org/covid19/
5. https://privacyinternational.org/examples/tracking-global-response-covid-19
6. White, S. (2020). Calculating and Reporting Healthcare Statistics, (6th ed.). Chicago, IL: AHIMA
7. https://irb.ucsf.edu/definitions
8. https://www.comparitech.com/blog/information-security/aggregate-vs-anonymous-data/
9. https://datascience.nih.gov/covid-19-open-access-resources
10. https://www.ecdc.europa.eu/en/covid-19-pandemic
11. https://www.forbes.com/sites/ciocentral/2020/03/30/big-data-in-the-time-of-coronavirus-covid-19/#5bb010b558fc
12. Lenert,L. Yeager McSwain, B.2020. Balancing health privacy, health information exchange, and research in the context of the COVID-19 pandemic. Journal of the American Medical Informatics Association, Volume 27, Issue 6, June 2020, Pages 963–966, https://doi.org/10.1093/jamia/ocaa039
13. McDonald, K. 2020. Paging service linked to medical data breach in WA. Pulse IT. Available at: https://www.pulseitmagazine.com.au/news/australian-ehealth/5611-paging-service-linked-to-medical-data-breach-in-wa
14. Lenert,L. Yeager McSwain, B.2020. Balancing health privacy, health information exchange, and research in the context of the COVID-19 pandemic. Journal of the American Medical Informatics Association, Volume 27, Issue 6, June 2020, Pages 963–966, https://doi.org/10.1093/jamia/ocaa039
15. https://abc13.com/covid-and-race-testing-houston-13-investigates/6329531/
16. https://www.chcf.org/blog/multiple-testing-issues-hamper-covid-19-response-nationwide/
17. https://vancouversun.com/news/long-lines-developing-to-get-covid-tests
18. See Eric Gay/AP Photo in https://abc13.com/covid-and-race-testing-houston-13-investigates/6329531/
19. https://www.hhs.gov/coronavirus/community-based-testing-sites/index.html
20. https://unitedstatesofcare.org/covid-19/state-covid-19-testing-landscape/
21. https://www.ehidc.org/resources/webinar-covid-19-contact-tracing-status-challenges-and-lessons-learned
22. https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/contact-tracing.html
23. https://www.pcmag.com/how-to/heres-how-contact-tracing-will-work-on-iphones-and-android-phones
24. https://www.ehidc.org/resources/webinar-covid-19-contact-tracing-status-challenges-and-lessons-learned
25. Ibid.
26. Office of the Information and Privacy Commissioner Alberta. Commissioner Comments on Alberta's Contact Tracing App May 1, 2020 https://www.oipc.ab.ca/news-and-events/news-releases/2020/commissioner-comments-on-alberta%E2%80%99s-contact-tracing-app.aspx
27. Office of the Information and Privacy Commissioner Alberta. ABTraceTogether Privacy Impact Assessment Review Report, Alberta Health and Alberta Health Services File 015714, July 2020 https://www.oipc.ab.ca/media/1089098/Report_ABTraceTogether_PIA_Review_Jun2020.pdf
28. Lifshitz, Lisa R. No free lunch: global privacy regulators set expectations of video teleconference providers. Canadian Lawyer Magazine. https://www.canadianlawyermag.com/news/opinion/no-free-lunch-global-privacy-regulators-set-expectations-of-video-teleconference-providers/331843. 24 Jul 2020
29. Lifshitz, Lisa R. No free lunch: global privacy regulators set expectations of video teleconference providers. Canadian Lawyer Magazine. https://www.canadianlawyermag.com/news/opinion/no-free-lunch-global-privacy-regulators-set-expectations-of-video-teleconference-providers/331843. 24 Jul 2020
30. Smith, E. and Macdonald, R., 2006. Managing Health Information during Disasters. Health Information Management Journal, 35(2), pp.8-13.
31. Mental Health Ramifications of COVID 19: The Australian Context (2020) Blackdoginstitute.org.au, Available from: https://www.blackdoginstitute.org.au/wp-content/uploads/2020/04/20200319_covid19-evidence-and-reccomendations.pdf (accessed 29 July 2020)
32. Durey A and Thompson S (2012) Reducing the health disparities of Indigenous Australians: time to change focus. BMC Health Services Research, 12(1).
33. Mental Health Ramifications of COVID 19: The Australian Context (2020)
34. Yussuf A (2020) The aftermath of Melbourne's housing tower lockdown: 'I don't know if I'm ever going to be the same again'. The Feed, Available from: https://www.sbs.com.au/news/the-feed/the-aftermath-of-melbourne-s-housing-tower-lockdown-i-don-t-know-if-i-m-ever-going-to-be-the-same-again (accessed 29 July 2020).
35. Waters J (2020) Is Mental Health the new pandemic. The Journal of the Health Visitors Association, 93(4), 34-39, Available from: http://dbgw.lis.curtin.edu.au:2048/login?url=https://search-proquest-com.dbgw.lis.curtin.edu.au/docview/2423571995?accountid=10382 (accessed 29 July 2020).
36. Vine R (2020) The Mental Health Impact of COVID 19. https://www.health.gov.au/news/the-mental-health-impact-of-covid-19, Available from: https://www.health.gov.au/news/the-mental-health-impact-of-covid-19 (accessed 29 July 2020).
37. OAIC (2020) COVID-19. Available from: https://www.oaic.gov.au/updates/news-and-media/covid-19/ (accessed 29 July 2020).
38. https://www.mygov.in/aarogya-setu-app/?app=aarogya&target=browser&t=1596870731
39. https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf
40. https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html
41. https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html
42. https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-community-based-testing-sites.pdf
43. https://www.hhs.gov/sites/default/files/guidance-on-media-and-film-crews-access-to-phi.pdf
44. https://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html