




Patient privacy in the COVID-19 era: Data access, transparency, rights, regulation and the case for retaining the status quo

Health Information Management Journal
2021, Vol. 50(1-2) 6–8
© The Author(s) 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1833358320966689
journals.sagepub.com/home/himj



Joan Henderson, BAppSc (HIM) (Hons 1), PhD (Med) 

Initiated in response to the COVID-19 pandemic, a range of new techniques and delivery processes have been developed that functionally change access to clinical care, and significantly challenge governance of information associated with these services. Many countries have overarching privacy legislation in place for protection of personal and patient information, but sudden and rapid changes to services (e.g. telehealth, COVID-19 testing stations, rapid access to pathology results, tracking apps) were introduced well ahead of any considered legal protections for patient privacy and governance of these processes.

Lenert and McSwain (2020) proposed changes to current regulations in the United States because they limit collaboration on patient care and research to constrain the virus and understand its sequelae. Similar regulatory protections for personal and health information exist in Australia (Office of the Australian Information Commissioner, 2020) at both state and federal levels. For more than a decade, researchers have criticised the limitations that these protections place on epidemiological research, arguing that processes such as obtaining consent cause time delays and reduce research efficiency; create selection bias (Tu et al., 2004); lack clarity in defining “de-identified,” “re-identifiable” and “non-identifiable”; and that, while there is little evidence of complaints or privacy breaches in health research (O’Keefe and Connolly, 2010), there is a real possibility for actual harm from lack of access to individual medical records by bona fide researchers (Peto et al., 2004). Privacy restrictions on linking disease registries with other necessary patient information is a further complication (Gun, 2005). Privacy, however, is a “qualified fundamental human right” (United Nations, 1948), requiring protection (Warren and Brandeis, 1890). The right to privacy and confidentiality for health information has a long history:

And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets. (Hippocrates (circa 320 BCE) in Jones (ed.), 1868)

An Australian Medical Association survey in 2005 found that patients had “strong concerns” about the privacy and security of their medical record information, even when de-identified. Their greatest reported concern was that their private health information could be sold for profit without their permission; 81% said their doctor should ask for permission before providing their de-identified medical information even for research (Australian Medical Association, 2005). More recent studies indicate that patient attitudes remain much the same (Kalkman et al., 2019). Patients may support sharing their health information for research, but their reservations remain high and their support conditional, due to concerns about privacy, security, control, responsibility and accountability.

Coronavirus has moved the goalposts. From a purely epidemiological perspective, there is an argument for privacy regulation “work-arounds” for the common good. In other circumstances (e.g. border closures, social distancing, compulsory mask-wearing) the rights of the individual are restricted, with limitations imposed for communal safety. The need for immediate patient information is imperative for contact tracing, public health reporting and appropriate, timely clinical care, but whether or not the pandemic has changed patient attitudes is unknown.

Historically, patients felt assured that their “physical” paper-based medical records were stored securely by their health professionals. This system had considerable limitations from a care provision perspective. Through digital transformation, patient data are increasingly aggregated, accessible and arguably less secure, in correlation with pressures on patients to accept imposed change. The result is a lack of trust and a general lack of confidence in the ability of well-meaning data recipients to provide adequate

The University of Sydney, Australia

Accepted for publication September 25, 2020.

Corresponding author:

Joan Henderson, Editor, *Health Information Management Journal*, Hon. Senior Research Fellow, The University of Sydney School of Public Health, Faculty of Medicine and Health, The University of Sydney, NSW 2006, Australia.

E-mail: joan.henderson@sydney.edu.au

protection to health data. At the performance level, some innovations have proved limited to the degree that the trade-off between privacy and access to information is unconvincing. For example, the Australian COVID-19 Tracing App introduced in April 2020 (Australian Government Department of Health, 2020), at a cost of more than Australian \$2 million (Sadler, 2020), has so far failed to locate anyone not found through manual tracing. Several reasons have circulated for its failure: it didn't function adequately with iPhones; contacts had to be within a 1.5-m radius for at least 15 minutes (surface contact transfer can occur in much less time). However, one of the main reasons was the low uptake. For the tracing app to be effective, around 60% of the population needed to be involved (Hinch et al., 2020), yet fewer than 25% of Australians download the app (Patton, 2020). The low participation possibly reflected a populace lacking confidence in their government's capacity to deliver something useful given their recent track record of problematic IT innovations: the 2016 Census ("crashed" in its first foray from paper to online format) (ABC News, 2016); the *My Health Record* (similarly "crashed" when online applications opened) (McCauley, 2018); and "Robo-debt" (significant computer-generated overpayments were erroneously raised against social security recipients) (Hayne and Doran, 2020). Another "trust" factor may be associated with the data from the tracing app being stored by a foreign company (Amazon Web Services) (Sadler, 2020).

The *My Health Record* initiative displayed similar participant uptake reluctance. After low "opt-in" registrations, the government changed tactics to "opt-out." Given its cost and potential, it seemed a logical move so that the majority of the population would benefit from the system. It is unknown whether the one-in-ten who opted out did so through pique (the removal of their option to join, based on an informed decision); through distrust of the government "owning" their health data; through concern that data can also be disclosed to law enforcement and other government agencies (Australian Government Department of Health, 2020); or that the government could not guarantee protection of their privacy from accidental breaches or deliberate hacking. Given these concerns, it appears reassuring that so few opted out, and 90% of Australians now have a *My Health Record* (Australian Digital Health Agency, 2019). However, as of January 2020, only 12.9 million (56.9%) of the 22.65 million records created had any content, and only 2.07 million (9.1%) records had been accessed by individual patients (Taylor and Corderoy, 2020). Public reluctance to become actively involved remains.

The two examples above required a high degree of transparency to reassure the population on governance issues, but COVID-19 has also boosted opportunities for other, less transparent commercial organisations to expand their markets. An increasing number of telehealth, appointment booking and pre-screening services present potential risk to privacy of which patients may not be aware. For example, HealthShare's BetterConsult for General Practitioners (GPs) (BetterConsult, 2020) is self-described as "a time saving pre-consultation tool that captures your patients'


symptoms, medication and other relevant clinical information. It then translates the data into concise medical notes, read for review before the consultation." General practices register with the service; when a patient books an appointment, the patient is sent "a secure link to a structured pre-consultation interview" (BetterConsult, 2020). This system is integrated into most of the leading GP clinical software products. It is not the first of its kind; HealthEngine has been in operation since 2006 and offers appointment connections to GPs, dentists and allied health professionals (HealthEngine, 2020a). The company recently released a report (based on a convenience sample of 730 practices) on the uptake of telehealth during April–June 2020 (HealthEngine, 2020b), which provided interesting feedback about who, how, where and why the (de-identified) respondent patients accessed telehealth care. These connection providers have potential to deliver positive and convenient services, but there are many questions unanswered in terms of governance and privacy protections for the data they collect. Both recommend that patients read their privacy policy and terms of use statements (collectively between 8000 and 11,000 words for each company) but how many patients will do so – or comprehend them? Pain is distracting, and over 65% of Australian GP-patient encounters involve management of a condition likely to be causing pain or distress at the time of their consultation; one in three are over 65 years of age, and 10% are from a non-English-speaking background (Britt et al., 2016). The amount of personal and health information collected through these platforms is comprehensive, and one of these companies has recently been fined Australian \$2.9 million "for publishing misleading patient reviews of medical practices and sharing patient contact information with private health insurance brokers," the latter having earned them more than Australian \$1.8 million (Bungard, 2020).

The lack of clarity around the governance of patient information collected through these systems raises other questions: Do patients feel obliged to use this service if they want to see the GP? Are they informed that it is not conditional? Might they feel that refusal may impact on the care they receive? Do they understand that this provider now "owns" whatever information they have entered or do they think this is part of their GP record? If they don't understand, how can this be considered "informed" consent for "secondary use" of their information? Are clinicians aware that the company is using preconsultation interview data, in what circumstances, possibly releasing it, to whom, and for how much? What are the medico-legal implications for the GP/practice if patients do not have full understanding and there is a complaint? Do the clinical professional organisations approve of their use? Have their Ethics Committees had any input? Ultimately, how informative are these datasets given they are non-probability (convenience) samples, unlikely to be representative of the population, and therefore not reliable sources for extrapolation of any analysed findings? It is paradoxical that so much is spent on "data" of such limited value when, in order to produce valid, reliable information, qualified researchers must demonstrate achievable

goals, rigorous methods and ethical scrutiny of their governance to win highly competitive funding.

This pandemic notwithstanding, the argument that patient privacy should be compromised for such minimal benefit is unconvincing. There is little advantage in easing legislative protections, and much to be gained by increasing privacy and governance restrictions on services making substantial financial gains from patient health information. Conversely, it is time to demand plain language explanations, ethical oversight and mandatory inclusion of personnel with knowledge and experience in the governance of health information, so patients, clinicians and the owners of these convenient services are all protected appropriately.

ORCID iD

Joan Henderson, BAppSc (HIM) (Hons 1), PhD (Med)  <https://orcid.org/0000-0002-8456-7455>

References

- ABC News (2016) Census 2016: ABS website crashes in #censusfail. Available at: <https://www.abc.net.au/news/2016-08-09/abs-website-inaccessible-on-census-night/7711652> (accessed 9 October 2020).
- Australian Digital Health Agency (2019) *Annual Report 2018–19*. Available at: <https://www.digitalhealth.gov.au/about-the-agency/publications/reports/annual-report/2018-19-australian-digital-health-agency-annual-report> (accessed 9 October 2020).
- Australian Government Department of Health (2020) COVID-Safe app. Available at: <https://www.health.gov.au/resources/apps-and-tools/covidsafe-app> (accessed 9 October 2020).
- Australian Medical Association (2005) AMA poll shows patients are concerned about the privacy and security of their medical records. Available at: <https://ama.com.au/media/ama-poll-shows-patients-are-concerned-about-privacy-and-security-their-medical-records> (accessed 9 October 2020).
- BetterConsult (2020) More time, more control and less admin for doctors. Available at: <https://au.betterconsult.com/> (accessed 9 October 2020).
- Britt H, Miller G, Henderson J, et al. (2016) *General Practice Activity in Australia 2015–16. General Practice Series No 40*. Sydney: Sydney University Press. Available at: <https://www.syddney.edu.au/medicine-health/our-research/research-centres/bettering-the-evaluation-and-care-of-health/publication.html> (accessed 9 October 2020).
- Bungard M (2020) Doctors booking site HealthEngine fined \$2.9 million for misleading patients. *The Sydney Morning Herald*, 20 August. Available at: <https://www.smh.com.au/business/consumer-affairs/doctor-booking-site-healthengine-fined-2-9-million-for-misleading-patients-20200820-p55noi.html> (accessed 10 October 2020).
- Gun R (2005) Privacy law is kneecapping epidemiological research. *Australasian Epidemiologist* 12(1): 2–4.
- Hayne A and Doran M (2020) Government to pay back \$721m as it scraps Robodebt for Centrelink welfare recipients. ABC News, 29 May. Available at: <https://www.abc.net.au/news/2020-05-29/federal-government-refund-robodebt-scheme-repay-debts/12299410> (accessed 10 October 2020).
- HealthEngine (2020a) Your home for healthcare. Available at: <https://healthengine.com.au/> (accessed 31 August 2020).
- HealthEngine (2020b) *The Uptake of Telehealth: HealthEngine Insights Report*. Available at: <https://he.app.link/telehealth-insights-2020-07> (accessed 10 October 2020).
- Hinch R, Probert W, Nurtay A, et al. (2020) *Effective Configurations of a Digital Contact Tracing App: A Report to NHSX*. The Fraser Group, University of Oxford. Available at: <https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown> (accessed 10 October 2020).
- Hippocrates in “The Oath,” Hippocrates Collected Works, Jones WHS (transl. and ed.) (1868) Cambridge: Harvard University Press. Available at: <https://daedalus.umkc.edu/hippocrates/HippocratesLoeb1/page.224.a.php?size=240x320> (accessed 10 October 2020).
- Kalkman S, van Delden J and Banerjee A, et al (2019) Patients’ and public views and attitudes towards the sharing of health data for research: a narrative review of empirical evidence. *Journal of Medical Ethics*. Epub ahead of print 12 November 2019. doi: 10.1136/medethics-2019-105651.
- Lenert L and McSwain BY (2020) Balancing health privacy, health information exchange, and research in the context of the Covid-19 pandemic. *Journal of the American Medical Informatics Association* 27(6): 963–966.
- McCauley D (2018) My Health Record opt-out deadline extended after system crash. *The Sydney Morning Herald*, 14 November. Available at: <https://www.smh.com.au/politics/federal/my-health-record-opt-out-deadline-extended-after-system-crash-20181114-p50g01.html> (accessed 10 October 2020).
- Office of the Australian Information Commissioner (2020) The Privacy Act 1988. Available at: <https://www.oaic.gov.au/privacy/the-privacy-act/> (accessed 10 October 2020).
- O’keefe CM and Connolly CJ (2010) privacy and the use of health data for research. *Medical Journal of Australia*, 193(9): 537–541.
- Patton L (2020) COVIDfail - the Australian coronavirus tracing app that can’t find anyone. *The NewDaily*, 8 July. Available at: <https://thenewdaily.com.au/news/national/2020/07/08/covid-fail-app/> (accessed 10 October 2020).
- Peto J, Fletcher O and Gilham C (2004) Data protection, informed consent, and research. *BMJ* 328: 1029–1030.
- Sadler D (2020) Big bucks on open source COVIDsafe app, 6 May. Available at: <https://www.innovationaus.com/big-bucks-on-open-source-covidsafe-app/> (accessed 10 October 2020).
- Taylor J and Corderoy A (2020) My Health Record: almost \$2bn spent but half the 23m records created are empty. *The Guardian*, 23 January. Available at: <https://www.theguardian.com/australia-news/2020/jan/23/my-health-record-almost-2bn-spent-but-half-the-23m-records-created-are-empty> (accessed 10 October 2020).
- Tu J, Willison D, Silver F, et al. (2004) Impracticability of informed consent in the Registry of the Canadian Stroke Network. *The New England Journal of Medicine* 350: 1414–1421.
- United Nations (1948) Universal Declaration of Human Rights, Article 12. Available at: <https://www.un.org/en/universal-declaration-human-rights/> (accessed 10 October 2020).
- Warren SD and Brandeis LD (1890) The right to privacy. *Harvard Law Review* 4(5): 193–220. JSTOR. Available at: www.jstor.org/stable/1321160 (accessed 14 September 2020).