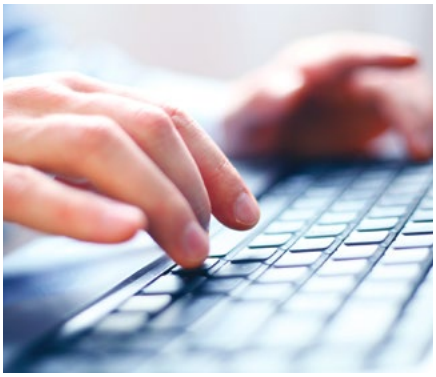
Privacy breaches and electronic communication

Lessons for practitioners and researchers



CPD

David J Carter, Samuel Hartridge

Background
In the era of socially distanced clinical and medical research practices, the use of electronic communication has flourished. The Australian Information Commissioner recently ordered a Victorian general practice to pay $16,400 in compensation following a breach of privacy. This is the largest award of compensation made by the Commissioner in the context of a medical or healthcare privacy matter. The practice had inadvertently sent an email containing sensitive information to an incorrect email address. The email included information concerning the human immunodeficiency virus status of the complainants.

Objective
The aim of this article is to provide an overview of this important case in Australian information and privacy law, which relates to the operation of an Australian general practice and research activity undertaken within the practice context.

Discussion
In an era marked by a great increase in the use of electronic communication in the medical setting, it is essential that practices both manage electronic communication well and respond appropriately when an error arises.

Interference with privacy

Use of electronic communication in the general practice setting is essential, and yet it generates significant medicolegal risk. The recent decision by the Australian Information Commissioner ('the Commissioner') illustrates this well. In this decision, the Commissioner determined that the Northside Clinic, a Victorian general practice, had interfered with the privacy of two complainants.[1] The Commissioner found that there was an unauthorised disclosure of sensitive information – including human immunodeficiency virus (HIV) status – and the practice had failed to take reasonable steps to protect the information that it held, in breach of Australian Privacy Principles.

The practice had intended to invite two patients to participate in medical research involving men who were HIV positive and in same-sex relationships in which one partner had been recently diagnosed with HIV. Both patients had earlier participated in a study facilitated by the practice. The practice sent an email addressed to the first patient's work email address and to an incorrect email address for the second patient, containing the second patient's first and last name but omitting their middle initial. The email disclosed the patients' names, the practice they were attending, their participation in an earlier HIV-related research study, their same-sex relationship and their HIV status. The email also disclosed the first patient's place of employment, personal and work email addresses, appointment information and his recently diagnosed HIV status.

Privacy law provides that health information cannot be disclosed unless the disclosure is consented to or is directly related to the primary purpose, or a permitted health situation exists.[2] In this case, none of those exceptions were present, so the unauthorised disclosure represented a breach of privacy law.

Practices are also required by law to take reasonable steps to protect personal information from unauthorised disclosures. The Commissioner found that the practice had failed to implement adequate privacy policies and procedures. While there was no evidence that such steps would have necessarily prevented the unauthorised disclosure, they would have decreased the likelihood that it would have occurred.

Compensation and damages

The complainants submitted that they were entitled to compensation in the amount of $250,000, arguing the impact of the disclosure and the practice's 'initial slow [and] blasé response [to the

disclosure] and lack of immediate action',[1] compounded by particular sensitivity of the information disclosed, warranted significant damages. The Commissioner's determination included an order to pay monetary compensation totalling $16,400 for both non-economic loss and economic loss arising due to the disclosure. This is the largest award of compensation ordered by the Commissioner in the context of health and medical services.

The compensation indicates a willingness to recognise non-economic loss, with the Commissioner paying great attention to the psychological impacts of the privacy breach. The first patient sought the assistance of a psychologist who, in reports furnished to the Commission, described the patient's presentation as 'shock, disbelief, anxious, shaken and outraged', subsequently coming to 'feel numb, disconnected, depressed [and] rejected'.[1] The patient was diagnosed with 'adjustment disorder with anxiety and depression in relation to the disclosure of his personal information'.[1] The psychological harm to the first patient led to award of compensation for non-economic loss totalling $10,000, while the cost of psychological treatment was compensated with award of compensation for economic loss of $3400. The second patient was awarded $3000 in compensation for non-economic loss.

Lessons for practices and practitioners: Responding swiftly and managing clinical care

The quantum of compensation awarded in *'SD' and 'SE' and Northside Clinic* should be measured against the steps that the practice had taken to remedy the authorised disclosure and to rectify its failure to protect the personal information it held. In fact, the Commissioner found that the handling of the breach by the practice may have exacerbated the impact of the breach itself in a range of ways.

Practices must respond swiftly to notice of a potential privacy breach. In *'SD' and 'SE' and Northside Clinic*, the practice failed to respond to their patient's email notifying them of the error. It took a second email from their patient alerting them that a complaint would be made to the Commissioner to elicit a response.

Practices must attempt to contain and rectify breaches. A rapid response presents an opportunity to remediate the breach and contain any further disclosure. The Commissioner found that the practice delayed attempted rectification. It took approximately one month until the practice attempted to contact the holder of the incorrect email address. A full four months elapsed until the practice provided notice of the disclosure to the company that managed the email address that was incorrectly emailed, requesting their assistance to rectify the disclosure.

A breach of privacy has potential to seriously damage the clinical relationship. Practices and health practitioners must ensure that the best interests of the patient remain paramount; that they execute their duty as health practitioners towards their patient, including disclosure of an adverse event; and that they provide appropriate support, including referral if needed, to support continuity of care. In this case, the Commissioner specifically noted the clinical elements of the breach. For example, the practice was said to have advised the first patient to seek psychological support in response to the breach. However, it was alleged that the practice failed to provide a referral or any support regarding that advice. Moreover, the patient was advised to seek a new treating doctor. The patient felt that they had been abandoned, and left with the impression that '[l]awyers [for the practice] suggest[ed] I find a new clinic for ongoing treatment' and that 'it became readily apparent that [the treating doctor] and [the practice] had abandoned me as a patient'.[1]

The conduct of the practice in this case can be compared with the conduct of the respondent psychologist in another recent healthcare email-related privacy breach, *'SF' and 'SG'*.[3] In that case, the respondent completely failed to take any remedial action or engage with the Office of the Australian Information Commission as it conducted its investigation. There the Commissioner awarded aggravated damages while noting that the conduct of the respondent in the case had been 'insulting towards the complainant and unjustified, demonstrating a disregard for the complainant's privacy rights ... [having] exacerbated the injury of the complainant by harming her proper feelings of dignity'.[3]

For its part, the practice in *'SD' and 'SE' and Northside Clinic* did eventually provide an unconditional apology to the patients, in so doing acknowledging the hurt and distress it had caused. It communicated that the complaint was not handled as well as it could have been and referred to changes to policy and procedure to prevent a recurrence. In response to the breach, the practice introduced a range of technical processes and operational procedures to improve its management of health information. These included a 'two-step authorisation' process for sending correspondence containing sensitive health information and the provision of privacy training for all employees. These measures were noted by the Commissioner. Had the practice failed to undertake these actions, it likely would have been ordered to implement remedial measures. Such measures would likely be accompanied by reporting obligations to the Commissioner's office.

The research context of this case is an interesting and important feature. The Commissioner did not make reference to the research study's governance structures, such as the relevant Human Research Ethics Committee (HREC). In failing to do so, it remains unclear as to what action may have been taken by the relevant HREC, what involvement or knowledge various members of the practice's clinical team may have had regarding the study or recruitment,[4,5] or how the study design and recruitment procedures may have influenced the action taken by the practice before and after the breach.

Conclusion

Any disclosure of health information outside that permitted by the law is an interference with the privacy of the individuals affected. Accordingly, medical practitioners and their practices must ensure effective policies and processes are implemented that reduce the likelihood that an unauthorised disclosure will occur.

This includes those regarding mandatory data breach requirements that have come into effect since the unauthorised disclosure made in *'SD' and 'SE' and Northside Clinic*.[6]

Failing to implement reasonable measures to protect information held and used by practices will itself constitute a further breach of privacy law and is a violation of *Good medical practice* (the code), where the high standards of professional conduct include 'protecting patients' privacy and right to confidentiality' and recognition that 'patients have a right to expect that doctors and their staff will hold information about them in confidence'.[7] In the same vein, the code outlines professional obligations that apply when ending a doctor–patient relationship when it becomes ineffective or compromised. This includes, importantly, a duty to inform the patient but also to facilitate handover and continuing care of the patient.[7]

Importantly, many of these legal and professional duties apply to the conduct of medical research. It is particularly important to ensure that research undertaken in clinical settings is managed in a manner that is mindful of the overlapping duties incumbent on clinicians and researchers, and regarding the provision of clinical services and the conduct of research.

Practices are advised to seek advice from privacy and health information management professionals, particularly in response to potential privacy or data breaches. The Royal Australian College of General Practitioners provides up-to-date guidance to medical practices regarding the management of privacy and health information in general practice,[8] as well as a clearly structured risk assessment tool for assessing the risks of current email practices and procedures,[9] while medical indemnity and other insurers will require disclosure and incident reporting be made.

Future reforms: More serious responses to privacy breaches

Lastly, it should be noted that the current Commonwealth privacy regime is undergoing review.[10] This will likely change the rules regulating the award of compensation for privacy violations. In its submission to the review, the Commissioner supported creation of additional remedies for invasions of privacy.[11] This included creation of a new statutory tort for serious invasions of privacy and a 'direct right of action' in the case of breaches of privacy. Both will allow individuals a direct right to bring actions in court rather than by a complaint lodged with the Commissioner. The Commissioner also recommended that compensation in such cases should not be capped. Accordingly, in the future, compensatory awards are likely to be significantly less 'restrained'.

Authors

David J Carter PhD (Law), LLM (Research), GradDip Legal Practice, BA (Communications), LLB (Hon I), Senior Lecturer, National Health and Medical Research Council Early Career Fellow, Faculty of Law, University of Technology, Sydney, NSW

Samuel Hartridge JD, GradDip Legal Practice, Allens Hub for Law, Technology and Innovation, Faculty of Law and Justice, University of New South Wales, NSW; Solicitor, KPMG Law, NSW

Competing interests: DJC is an Australian legal practitioner and legal academic who serves as a member of the governing body of the HIV/AIDS Legal Centre, a not-for-profit community legal centre.

Funding: This research was funded by the National Health and Medical Research Council (NHMRC) Early Career Fellowship Grant (Grant ID: 1156520). The contents are solely the responsibility of the individual author and do not reflect the views of the NHMRC.

Provenance and peer review: Not commissioned, externally peer reviewed

Correspondence to:
david.carter@uts.edu.au

References

1. 'SD' and 'SE' and Northside Clinic (Vic) Pty Ltd [2020] AICmr 21.
2. Commonwealth of Australia. Privacy Act 1988. Canberra, ACT: Commonwealth of Australia, 1988.
3. 'SF' and 'SG' (Privacy) [2020] AICmr 22.
4. Fraser J. A case report: Ethics of a proposed qualitative study of hospital closure in an Australian rural community. Fam Pract 2004;21(1):87–91. doi: 10.1093/fampra/cmh119.
5. Fraser J, Alexander C. Publish and perish: A case study of publication ethics in a rural community. J Med Ethics 2006;32(9):526–29. doi: 10.1136/jme.2005.014076.
6. Carter DJ, Hartridge S. Mandatory data breach notification requirements for medical practice. Med J Aust 2018;209(5):204–05. doi: 10.5694/mja17.00577.
7. Medical Board of Australia. Good medical practice: A code of conduct for doctors in Australia. Canberra, ACT: Medical Board of Australia, 2014.
8. The Royal Australian College of General Practitioners. Privacy and managing health information in general practice. East Melbourne, Vic: RACGP, 2017. Available at www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Protecting%20practice%20information/Privacy-and-managing-health-information-in-general-practice.pdf [Accessed 7 February 2021].
9. The Royal Australian College of General Practitioners. Fact sheet: Using email in general practice. East Melbourne, Vic: RACGP, 2017. Available at www.racgp.org.au/running-a-practice/technology/business-technology/using-email-in-general-practice [Accessed 1 June 2022].
10. Attorney-General's Department, Australian Government. Privacy Act review: Issues paper. Canberra, ACT: The Australian Government, 2020. Available at www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf [Accessed 7 February 2021].
11. Falk A (Australian Information Commissioner and Privacy Commissioner). Privacy Act review – Issues paper: Submission by the Office of the Australian Information Commissioner. Sydney: 2020. Available at www.ag.gov.au/sites/default/files/2021-01/office-of-the-australian-information-commissioner.PDF [Accessed 1 June 2022].

correspondence **ajgp@racgp.org.au**