MANDATORY DATA BREACH NOTIFICATION LAWS AND AUSTRALIAN HEALTH DATA PRIVACY: FRAGMENTS AND FAULT LINES

MEGAN PRICTOR*

Data privacy breaches — unauthorised access to, disclosure, or loss of people's personal information — are commonplace, particularly in the health sector. In Australia, provisions under the Privacy Act 1988 *(Cth) and the* My Health Records Act 2012 *(Cth) require data breach notification to affected people and the regulator. However, this mandatory notification, as it pertains to health information, has two key problems: fragmentation, and lack of fitness for purpose. In this article, I analyse the goals of the Australian legislative developments and the extent to which these are met in relation to health data. I propose legal and procedural reforms to mend the fragments and fault lines so that breach notification can more effectively address healthcare data breaches in Australia.*

I INTRODUCTION

A *Health Data Breaches*

Unauthorised access to, disclosure, or loss of people's personal information — known as data privacy breaches — are commonplace internationally. They occur in relation to all types of personal data including health information. Data breaches are not simply a consequence of data proliferation driven by exponential digitisation. Traditional medical record systems that use paper files and fax machines are also subject to data privacy breaches. In September 2019, a report emerged that a Melbourne medical clinic had repeatedly, albeit accidentally, faxed sensitive details of approximately ten patients, intended as referrals to a specialist, to a wrong number over the preceding two years.[1] These referrals included details of patients' mental health conditions, personal circumstances, prescribed

* Senior Lecturer, Health, Law and Emerging Technologies programme, Melbourne Law School, The University of Melbourne.

1 Melissa Cunningham, '"Detailed and Graphic": Clinic Faxes Patients' Highly Sensitive Medical Histories to Wrong Number', *The Age* (online, 18 September 2019) <https://www.theage.com.au/national/victoria/detailed-and-graphic-clinic-faxes-patients-highly-sensitive-medical-histories-to-wrong-number-20190916-p52rsy.html>.

medications, and names and contact information including home addresses. In another example, paper records of patients at a Melbourne private hospital were found in the street by a passer-by.[2] They contained information on do-not-resuscitate orders, surgeries, diagnoses, and medications. The person who discovered the documents was reportedly 'shocked to receive no guarantee the hospital would tell the patients about the breach'.[3] At the time of these data breaches, there was no legal requirement in Australia that an organisation must inform those affected about a breach of their data privacy, even where personal health information was revealed. Since then, the legal landscape has changed, but not in a way that necessarily makes most sense for health data.

Although most data breaches affect only a small number of people,[4] large-scale breaches also occur. People in Singapore suffered one of the most egregious breaches, when in June 2018 the SingHealth system was maliciously accessed by persons unknown. As well as the medication records of 160,000 patients, the non-medical personal information of 1.5 million patients was copied. This information included 'name, national identification number, address, gender, race, and date of birth'.[5] Other major health data breaches in recent years include those affecting the Australian Red Cross Blood Service (550,000 people),[6] the French Mutuelle Generale de la Police health insurance database (112,000 people),[7] the United States-based Quest Diagnostics (34,000 people),[8] and the United States HealthCare.Gov portal (75,000 people).[9] There are fears about a cyber-attack on

2 Julia Medew, 'Dozens of Patients' Medical Records Found Lying in Melbourne Street', *The Age* (online, 26 March 2017) <https://www.theage.com.au/national/victoria/dozens-of-patients-medical-records-found-lying-in-melbourne-street-20170324-gv62op.html>.

3 Ibid.

4 See, eg, Office of the Australian Information Commissioner, *Notifiable Data Breaches Scheme 12-Month Insights Report* (Report, 13 May 2019) 5, 14 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/> ('*Notifiable Data Breaches Scheme*').

5 Eileen Yu, 'Singapore Suffers "Most Serious" Data Breach, Affecting 1.5M Healthcare Patients Including Prime Minister', *ZDNet* (online, 20 July 2018) <https://www.zdnet.com/article/singapore-suffers-most-serious-data-breach-affecting-1-5m-healthcare-patients-including-prime/>.

6 David Glance, 'Questions Still Need Answering in Australia's Largest Health Data Breach', *The Conversation* (online, 31 October 2016) <http://theconversation.com/questions-still-need-answering-in-australias-largest-health-data-breach-67916>.

7 'French Police Hit by Security Breach as Data Put Online', *BBC News* (online, 27 June 2016) <https://www.bbc.com/news/world-europe-36645519>.

8 Quest Diagnostics, 'Quest Diagnostics Provides Notice of Data Security Incident' (News Release, 12 December 2016) <https://newsroom.questdiagnostics.com/2016-12-12-Quest-Diagnostics-Provides-Notice-of-Data-Security-Incident>.

9 Dell Cameron, 'HealthCare.Gov Portal Suffers Data Breach Exposing 75,000 Consumers', *Gizmodo* (online, 19 October 2018) <https://gizmodo.com/healthcare-gov-portal-suffers-data-breach-trump-offici-1829877392>.

Australia's national My Health Record system,[10] which now holds extensive health records and other personal information of approximately 23 million Australians.[11] This was underscored in mid-2020 when the Australian Department of Foreign Affairs and Trade and the Australian Cyber Security Centre issued a joint statement about cybersecurity threats amid the COVID-19 pandemic, noting that 'reports that malicious cyber actors are seeking to damage or impair the operation of hospitals, medical services and facilities' were of particular concern.[12]

B *Data Breach Notification*

Various legal and procedural responses are available to address the issue of data security failures. This paper focuses on data breach notification, that is, telling a person that their personal information has been subject to unauthorised access, unauthorised disclosure, or loss.[13] I use the term 'notification' to describe communication to individuals whose data have been subject to a breach. The terms 'reporting' and 'advice' are used to describe a regulatory authority being informed about a breach. 'Notification schemes' overall may incorporate both of these activities. Breach notification as a legal requirement for personal data management first emerged in the United States ('US') in California in 2002 and is slowly being adopted internationally.[14] In Europe, amendments to the *Directive on Privacy and Electronic Communications* ('*ePrivacy Directive*') introduced personal data breach notifications to the telecommunications sector.[15] This was extended in 2018

10 Chris McCall, 'Opt-Out Digital Health Records Cause Debate in Australia' (2018) 392(10145) *Lancet* 372.

11 Australian Digital Health Agency, *Statistics and Insights: July 2022* (Report, July 2022) 2 <https://www.digitalhealth.gov.au/sites/default/files/documents/my-health-record-statistics---july-2022.pdf>

12 Australian Department of Foreign Affairs and Trade and Australian Cyber Security Centre, 'Unacceptable Malicious Cyber Activity' (Joint Statement, 20 May 2020) <https://www.dfat.gov.au/news/news/unacceptable-malicious-cyber-activity>.

13 Other responses include: investigation by a regulator — in Australia, this is the Office of the Australian Information Commissioner or equivalent state-based authorities — which may result in an enforceable undertaking (*Privacy Act 1988* (Cth) s 80V), a determination (s 52), injunction (s 80W) or civil penalty order (s 80U). A company might institute protective measures on a person's behalf (eg monitoring of their account, requiring them to change passwords). In Australia, there have been repeated calls for the introduction of a tort of invasion of privacy to enable individuals to seek restitution for harms caused by data and other privacy breaches: Australian Law Reform Commission, *Serious Invasion of Privacy in the Digital Era* (Final Report No 123, June 2014); Law Council of Australia, 'Law Council Supports Statutory Tort for Serious Invasion of Privacy' (Media Release, 8 February 2022) <https://www.lawcouncil.asn.au/media/media-releases/law-council-supports-statutory-tort-for-serious-invasion-of-privacy>.

14 Nicholas Blackmore, 'Mandatory Data Breach Notification Laws Spread across Asia Pacific', *Kennedys* (Web Page, 2 March 2018) <https://kennedyslaw.com/thought-leadership/article/mandatory-data-breach-notification-laws-spread-across-asia-pacific/>.

15 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)* [2002] OJ L 201/37, para 20, art 4(2) ('*ePrivacy Directive*').

by the *General Data Protection Regulation* ('*GDPR*') to all data controllers and data processors in all sectors.[16] Across Asia, South Korea, the Philippines, mainland China, Indonesia and Taiwan have notification requirements, although these vary in specificity.[17] New Zealand's *Privacy Act 2020* (NZ) includes mandatory breach notification provisions.[18] Both the Organisation for Economic Co-operation and Development ('OECD') and the Asia-Pacific Economic Cooperation ('APEC') endorse breach notification schemes for reasons that include promoting accountability and openness, enhancing the evidence base for managing privacy risks, and enabling individuals to protect themselves from consequences of a breach.[19] The OECD notes, however, that too little is currently known about the effects of breach notification.[20]

C *Mandatory Breach Notification to Data Subjects in Australia*

Mandatory notification in Australia is relatively new. Although first proposed in 2007,[21] and recommended by the Australian Law Reform Commission ('ALRC') in 2008,[22] it became law only in early 2018 with the commencement of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) amending the *Privacy Act 1988* (Cth) ('*Privacy Act*'). The notifiable data breach scheme, which forms pt IIIC of the *Privacy Act*, requires that an entity that is subject to the Act must advise the Information Commissioner and notify the affected individual if: '(a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and (b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates'.[23] Entities have up to 30 days to investigate a suspected breach before making any report or

16 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1, arts 3, 34 ('*GDPR*').

17 Blackmore (n 14).

18 *Privacy Act 2020* (NZ) ss 112–22.

19 Organisation for Economic Co-operation and Development, *The OECD Privacy Framework* (Report, 2013) 26 <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> ('*OECD Privacy Framework*'); Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (Report, 2015) 10–11.

20 *OECD Privacy Framework* (n 19) 27.

21 Privacy (Data Security Breach Notification) Amendment Bill 2007 (Cth).

22 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 1, 61 [51–1] <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/> ('*For Your Information*').

23 *Privacy Act 1988* (Cth) s 26WA ('*Privacy Act*').

notification,[24] and are absolved entirely of the need to do so if they take sufficient remedial action.[25]

It is important to note that the *Privacy Act* is not universally applicable in Australia, and hence nor is the federal breach notification scheme. Outside its scope are state and territory authorities, including state government departments, and bodies established for a public purpose under a state law (such as universities and public hospitals).[26] Their exclusion has significant consequences for the regulation and management of health data in Australia. Public hospitals, for instance, are largely exempt from mandatory breach notification requirements. They are subject to the *Privacy Act* notification scheme only in relation to records containing tax file numbers.[27] Further, two nationwide electronic health record systems that operate across, and contain data from, both the public and private sectors are subject to mandatory breach notification under tailor-made Commonwealth laws. The first of these is the My Health Record system established under s 75 of the *My Health Records Act 2012* (Cth) ('*My Health Records Act*'), while the second is the National Cancer Screening Register with s 22A of its *National Cancer Screening Register Act 2016* (Cth). This latter Register contains a comparatively limited data set that will not be discussed further here.

There are two main difficulties with the current approach to health-related data breach notification under Australian law. The first, that of fragmentation, is a clear reflection of Australia's federal system and the division of responsibility for the provision of health care between Commonwealth and state governments. Although this is by no means a novel legal problem in the Australian context, it presents a particular challenge to individuals receiving health care when they unwittingly traverse jurisdictional boundaries in utilising different commonly accessed health services. For instance, in quick succession a person might deal with a private general practitioner ('GP') (subject to both state and Commonwealth law), a state-administered public hospital (subject to state law but largely not the Commonwealth *Privacy Act*) and the federal government-administered My Health Record system that contains data from both jurisdictions (subject to the Commonwealth *My Health Records Act*). Health services themselves also experience unwelcome complexity as they must navigate different laws and breach notification procedures when they manage patient data in the My Health Record system compared with their other medical record systems. The problem of fragmentation has been previously noted mainly in the context of transnational data flows,[28] to which the OECD, APEC and other frameworks are a direct response. The effects of this fragmentation on both organisations and people receiving health care in Australia have not yet been considered in detail.

24 Ibid s 26WH.

25 Ibid s 26WF.

26 Ibid s 6 (definition of 'APP entity').

27 Ibid ss 26WB, 26WE(1)(d).

28 See, eg, Angela Daly, 'The Introduction of Data Breach Notification Legislation in Australia: A Comparative View' (2018) 34(3) *Computer Law and Security Review* 477.

The second difficulty, which I label 'fitness for purpose', relates to the design of mandatory breach notification schemes themselves, their 'underlying conceptual complexity'[29] and their comparative inability to address the harms caused by data breaches of health information in particular — compared with other types of personal information loss. The emergence of breach notification as a practice in response primarily to the theft of financial data has resulted in a notification scheme geared towards reducing identity theft and personal financial loss.[30] By comparison, the harms resulting from health data loss might tend instead towards psychological distress, embarrassment and stigma. Hence, the suitability of data breach notification as a legislated response in this arena must be examined; particularly given the administrative burden it imposes on organisations.

In this article, I will first examine the prevalence and nature of health data breaches in Australia. I will consider the issues of fragmentation and fitness for purpose through a detailed qualitative analysis of what the Australian legal developments have been designed to achieve, and whether they have met, their goals in relation to health data. I will posit responses to the identified issues by way of legal and procedural reforms including more comprehensive, informative and cohesive reporting of data breaches.

II THE NATURE AND EXTENT OF HEALTH DATA BREACHES IN AUSTRALIA

We do not know how many data breaches there were in Australia before the introduction of mandatory data breach notification in early 2018. Nor do we know the current extent of underreporting. The Office of the Australian Information Commissioner ('OAIC'), which receives reports of data breaches under the *Privacy Act*, received 1,132 such reports in the first year of the mandatory breach notification scheme (April 2018 to March 2019), of which 964 reported incidents met the definition of an 'eligible data breach'[31] (the remaining 168 being voluntary notifications).[32] Health services were the most likely sector to advise of a breach, with 206 reported over the period.[33] Data breaches of health information specifically (across all sectors) resulted in 249 reports to the OAIC (compared with, for instance, 833 reports for breaches related to contact information for the period).[34] In the health sector, human error (such as information emailed or posted to the wrong recipient, the loss of paperwork, or insecure data disposal) was the

29 Bill Lane et al, 'Stakeholder Perspectives regarding the Mandatory Notification of Australian Data Breaches' (2010) 15(2) *Media and Arts Law Review* 149, 167.

30 Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 16 [72].

31 *Privacy Act* (n 23) s 26WE(2)(c).

32 *Notifiable Data Breaches Scheme* (n 4) 8.

33 Ibid 13.

34 Ibid 14.

leading cause of data breaches advised to OAIC.[35] This mirrors patterns overseas; for instance, in the United Kingdom, recent quarterly reports by the Information Commissioner's Office show that health has often been the largest sector for breach notification, with non-cyber incidents vastly outweighing the number of breaches caused by cyber-attack.[36] The healthcare sector is clearly at high risk of notifiable data breaches, which likely reflects factors such as the volume of data assets and processing activities in health care as well as the sensitive nature of much of the data, making it attractive for cybercriminals. As US researchers noted, this sector

> has lagged behind other industries in protecting its main stakeholder (ie, patients), and now hospitals must invest considerable capital and effort in protecting their systems. However, this is easier said than done because hospitals are extraordinarily technology-saturated, complex organizations with high end point complexity, internal politics, and regulatory pressures.[37]

The problem in Australia, however, runs deeper than even the available data suggests. A report by BDO Australia indicated that fewer than 10% of the organisations responding to their survey who experienced a data breach in 2018 and were subject to the notifiable data breach scheme had advised the OAIC of the breach.[38] Entities subject to the scheme range from major private hospitals, aged and palliative care providers, to individuals such as specialists, GPs and allied health practitioners.[39] It is possible that individual practitioners with limited resources are unaware of their reporting obligations or ill-equipped to act upon them. Hence, more — perhaps many more — breaches are likely to have occurred than have been advised to the regulator.

Another reason that the OAIC reports offer an incomplete picture is that they omit the data breaches that occurred in state-based public health services. Public hospitals are not required by law to advise a regulator or notify affected individuals of data breaches (except those relating to tax file numbers or the My Health Record system).[40] This is despite the fact that many more people are admitted to public hospitals than private hospitals (7 million versus 4.9 million admissions in 2020–

35 Ibid 13.

36 'Data Security Incident Trends', *Information Commissioner's Office* (Web Page) <https://ico.org.uk/action-weve-taken/data-security-incident-trends/>.

37 Mohammad S Jalali and Jessica P Kaiser, 'Cybersecurity in Hospitals: A Systematic, Organizational Perspective' (2018) 20(5) *Journal of Medical Internet Research* e10059 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/>.

38 BDO and AUSCERT, *2018/2019 Cyber Security Survey* (Report, 2019) 17 <https://www.bdo.com.au/en-au/cyber-security/2018-2019-cyber-security-survey-results> ('*Cyber Security Survey*').

39 *Privacy Act* (n 23) ss 6D(4)(b), 6FB(3)(b).

40 Office of the Australian Information Commissioner, *Data Breach Preparation and Response* (Guide, July 2019) 24 <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response>.

1).[41] Given that, by sector, private health services lead mandatory notifications under the Commonwealth scheme, it is reasonable to extrapolate that data breaches are also a significant problem in the state public hospital sector. This suggestion is given further credence by two reports from the Victorian Auditor-General's Office, indicating that the state's public hospitals were dogged by longstanding and significant IT system security problems.[42] These problems included systems that were unsupported or outdated, access management that was unsatisfactory, and policies that were incomplete, combining to 'increase the likelihood of unauthorised access to hospitals' IT systems'.[43] In September 2019, several Victorian hospitals suffered a ransomware attack that affected various information technology ('IT') systems and resulted in the cancellation of appointments and surgeries, although apparently no patient data were compromised.[44] For these reasons — the relative newness of the Commonwealth scheme, its failure to cover state public sector entities, and the known existence of problems in state healthcare IT — data breaches of personal health information in Australia are likely to be far more numerous than the OAIC analyses suggest.

A *Data Breaches of the My Health Record System*

Data breaches affecting the My Health Record system are summarised annually by the Australian Digital Health Agency ('ADHA') — which operates the system — and the OAIC. The details of these breaches are provided in subsections of larger reports about digital health more broadly. By comparison, the breaches reported to the OAIC under the notifiable data breach scheme are the exclusive subject of specific OAIC summaries every six months. In the 2018–19 period, ADHA advised the OAIC of only four data breaches in connection with the My Health Record system, affecting four healthcare recipients.[45] The Chief Executive of Medicare advised the OAIC of a further 31 data breaches affecting 61 healthcare recipients; of whom 36 had a My Health Record at the time of the data breach.[46]

41 Australian Institute of Health and Welfare, *Australia's Hospitals at a Glance* (Web Report, 29 July 2022) <https://www.aihw.gov.au/reports/hospitals/australias-hospitals-at-a-glance/contents/hospital-activity>.

42 Victorian Auditor-General's Office, *Security of Patients' Hospital Data* (Report, May 2019) 31 <https://www.audit.vic.gov.au/sites/default/files/2019-05/29052019-Hospital-Data-Security.pdf>; Victorian Auditor-General's Office, *Results of 2016–17 Audits: Public Hospitals* (Report, November 2017) 26 <https://www.audit.vic.gov.au/sites/default/files/2017-11/20171129-Public-Hospitals-16%E2%80%9317.pdf> ('*Results of 2016–17 Audits*').

43 Victorian Auditor-General's Office, *Results of 2016–17 Audits* (n 42) 26.

44 'Victorian Hospitals across Gippsland, Geelong and Warrnambool Hit by Ransomware Attack', *ABC News* (online, 1 October 2019) <https://www.abc.net.au/news/2019-10-01/victorian-health-services-targeted-by-ransomware-attack/11562988?nw=0>.

45 Office of the Australian Information Commissioner, *Annual Report of the Australian Information Commissioner's Activities in Relation to Digital Health: 2018–19* (Report, 2019) 12 <https://www.oaic.gov.au/__data/assets/pdf_file/0020/9263/digital-health-annual-report-2018-19.pdf>.

46 Ibid.

Breaches of the My Health Record system to date appear to have mainly stemmed from fraudulent activity or system error rather than human error or cyber attack.[47] In 2019, a report by Australia's Auditor-General on the implementation of the system found that management of the cybersecurity risks relating to sharing data with third-party software vendors and healthcare providers (as opposed to risks pertaining to the core infrastructure) was inappropriate, and that oversight of these risks was lacking.[48] Human error or cyber-attack may become greater threats to the My Health Record system as there is an increase in the use of the system by healthcare providers and patients, and as its data holdings grow.

In summary, breaches of personal health data are common in Australia, potentially affecting thousands or tens of thousands of people each year.[49] There is a substantial knowledge gap as a consequence of the fragmented jurisdictional landscape of both breach notification to data subjects and reporting to regulators. The widespread nature of the problem, the sensitivity of personal health information (for instance, details about embarrassing or stigmatised medical conditions) and the harms that may result from data breaches in this sphere combine to heighten the need for robust and effective responses. A current impediment to this, the fragmented legal framework, will now be analysed in detail. In particular, I will consider the impact of this fragmentation on patients and healthcare providers, as well as on regulators' capacity to learn from data breaches to design more responsive ways to address them.

III LEGISLATIVE FRAGMENTATION AND ITS EFFECTS ON HEALTH-RELATED DATA BREACH NOTIFICATION IN AUSTRALIA

The interaction between Australian health systems and the available mandatory data breach notification provisions is set out in Table 1 below. State and territory privacy and health records laws, applying to state and territory public sector entities like hospitals and universities (as well as private sector entities), do not require notification to data subjects nor reporting to a regulator after a data breach.[50] In two jurisdictions (Western Australia ('WA') and South Australia),

47 Ibid.

48 Australian National Audit Office, *Implementation of the My Health Record System* (Performance Audit Report No 13, 25 November 2019) 9 <https://www.anao.gov.au/work/performance-audit/implementation-the-my-health-record-system>.

49 *Notifiable Data Breaches Scheme* (n 4) 14.

50 'Privacy Breach Management and Notification', *Office of the Information Commissioner Queensland* (Web Page, 3 February 2022) <https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/privacy-breach-management-and-notification>; Government of Western Australia, 'Privacy and Responsible Information Sharing: For the Western Australian Public Sector' (Discussion Paper, 2 August 2019) 31 <https://www.wa.gov.au/system/files/2021-08/Discussion%20paper_Privacy%20and%20

there is no overarching privacy legislation.[51] New South Wales ('NSW') has seen at least two previous attempts to implement mandatory notification. Following a consultation in 2019, the NSW Attorney-General made a commitment in March 2020 to introduce such a scheme under amendments to the *Privacy and Personal Information Protection Act 1998* (NSW).[52] WA and Queensland are also considering implementing a mandatory breach notification regime.[53] There have been calls for such a scheme in the Victorian public sector.[54] In the absence of mandatory schemes, most state and territory governments take an approach that encourages public sector agencies to notify affected people of data breaches,[55] while WA and Tasmania at present provide no guidance. Hence, a person attending a public hospital in any Australian state might experience the scenario described at the beginning of this article; their paper medical records might be picked up in the street, revealing deeply personal details to the finder, entirely without any requirement that they be notified.

Responsible%20Information%20Sharing_1.pdf> ('Privacy and Responsible Information Sharing'); Department of the Premier and Cabinet (SA), *Personal Information Data Breaches Guideline* (Guide, February 2018) 2 <https://www.dpc.sa.gov.au/__data/assets/pdf_file/0009/47394/Personal-Information-Data-Breaches.pdf> ('*Personal Information Data Breaches*').

51 'Privacy and Responsible Information Sharing' (n 50) 11.

52 Justin Hendry, 'NSW Govt Pledges to Introduce Mandatory Data Breach Reporting', *itnews* (online, 10 March 2020) <https://www.itnews.com.au/news/nsw-govt-pledges-to-introduce-mandatory-data-breach-reporting-539109>; 'Proposed Changes to NSW Privacy Laws', *NSW Government Communities and Justice* (Web Page, 1 October 2021) <https://www.justice.nsw.gov.au/justicepolicy/Pages/lpclrd/lpclrd_consultation/proposed-changes-to-nsw-privacy-laws.aspx>. This was finally implemented in the *Privacy and Personal Information Protection Amendment Act 2022* (NSW), which commences in November 2023.

53 'Privacy and Responsible Information Sharing' (n 50) 6–7; Justin Hendry, 'Qld Gov Proposes Mandatory Data Breach Reporting for Agencies', *itnews* (online, 24 June 2022) <https://www.itnews.com.au/news/qld-gov-proposes-mandatory-data-breach-reporting-for-agencies-581815>.

54 Joseph Brookes, 'Watchdog Calls for Mandatory Data Breach Notification Laws in Victoria', *InnovationAus.com* (Web Page, 15 September 2022) <https://www.innovationaus.com/watchdog-calls-for-mandatory-data-breach-notification-laws-in-victoria/>; Victorian Ombudsman, *Investigation into a Former Youth Worker's Unauthorised Access to Private Information about Children* (Report, September 2022) 49, 74 <https://assets.ombudsman.vic.gov.au/assets/VO-PARLIAMENTARY-REPORT_JONES_Sep-2022.pdf>.

55 'Contain and Communicate Privacy Breaches: Guidance for Northern Territory Public Sector Organisations', *Information Commissioner Northern Territory* (Web Page) <https://infocomm.nt.gov.au/__data/assets/pdf_file/0014/501710/Privacy-Breaches-Tip-Sheet-NT.pdf> ('Contain and Communicate'); *Personal Information Data Breaches* (n 50) 2; 'Managing the Privacy Impacts of a Data Breach', *Office of the Victorian Information Commissioner* (Web Page) <https://ovic.vic.gov.au/book/managing-the-privacy-impacts-of-a-data-breach/>; Information and Privacy Commission (NSW), *Data Breach Guidance for NSW Agencies* (Guide, May 2018) 7 <https://www.ipc.nsw.gov.au/sites/default/files/2020-03/Data_Breach_Guidance_for_NSW_Agencies_May_2018.pdf>; 'Privacy in the ACT', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/privacy/privacy-in-your-state/privacy-in-the-act>; 'Privacy Breach Management and Notification' (n 50).

Table 1. Australian Legislation Governing Health Data Breach Notification

Information system	*Jurisdiction*	*Principal legislation*	*Mandatory data breach notification provisions*	*Definition of notifiable breach*
My Health Record	Commonwealth	*My Health Records Act 2012* (Cth)	s 75	s 75(1)(b) '(i) a person has, or may have, contravened this Act in a manner involving an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record; or (ii) an event has, or may have, occurred (whether or not involving a contravention of this Act) that compromises, may compromise, has compromised or may have compromised, the security or integrity of the My Health Record system; or (iii) circumstances have, or may have, arisen (whether or not involving a contravention of this Act) that compromise, may compromise, have compromised or may have compromised, the security or integrity of the My Health Record system'
Private practitioner record	Commonwealth and state or territory	*Privacy Act 1988* (Cth)	pt IIIC (ss 26WA–26WT)	s 26WE '(2) For the purposes of this Act, if: (a) both of the following conditions are satisfied: (i) there is unauthorised access to, or unauthorised disclosure of, the information; (ii) a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or (b) the information is lost in circumstances where: (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and (ii) assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to

				any of the individuals to whom the information relates; then: (c) the access or disclosure covered by paragraph (a), or the loss covered by paragraph (b), is an ***eligible data breach*** of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; and (d) an individual covered by subparagraph (a)(ii) or (b)(ii) is ***at risk*** from the eligible data breach.'
		Health Records Act 2001 (Vic) or equivalent in other states and territories	Breach notification encouraged but not mandatory[56]	n/a
Public hospital record	State or territory	*Health Records Act 2001* (Vic) or equivalent in other states and territories	Breach notification encouraged but not mandatory[57]	n/a

There are important differences between the operation of the breach notification schemes set out in the *Privacy Act* and the *My Health Records Act*.[58] These differences include: the legal threshold for notification (as shown in Table 1), which entity has responsibility for notifying data subjects, and which agency must be advised. For the My Health Record system, the agency that must be advised also depends on whether the reporting entity is a state or territory authority, or not. In the event of a breach, the notification process depends upon which entity has suffered the breach. If ADHA is the entity, it reports to the OAIC. A state or territory authority is required to report a breach to ADHA. Another entity (such as a GP) must report to both the OAIC and ADHA in relation to a breach of the My Health Record system.

Unlike the *Privacy Act* provisions, there is no 'serious harm' threshold for breach notification in relation to the My Health Record system. If the event or

56 See above n 55.

57 See above n 55.

58 'Data Breach Action Plan for Health Service Providers', *Office of the Australian Information Commissioner* (Web Page, 11 February 2020) <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-action-plan-for-health-service-providers>.

circumstances described in s 75(1)(b) of the *My Health Records Act* occur, ADHA must notify all affected healthcare recipients and potentially also the general public (s 75(6)(c)–(d)). There is no legal requirement for any entity other than ADHA to notify the healthcare recipient directly, even if, for instance, a healthcare provider is directly responsible for the data breach.[59] If a breach relates to data that have been downloaded into another system, such as a hospital's electronic medical record ('EMR'), then the notification provisions of the *My Health Records Act* will not apply even though the data were derived from the My Health Record system.[60] In such a case, a public hospital would have no legal obligation to report the breach, whereas a private hospital would have such an obligation under the *Privacy Act*.

This fragmentation of data breach notification laws in Australian health care raises three important challenges, referred to earlier. First, it leads to inconsistency in notification practices that affects healthcare consumers. Second, it is likely to cause confusion to providers who must navigate these systems. Third, it results in an incomplete picture of the nature and extent of data breaches affecting the Australian healthcare sector as a whole, with consequences for the design of preventive and remedial activities. These issues will now be explored in further detail.

The following scenario illuminates the potential effect of fragmentation on the patient experience. A person visits their GP in Melbourne, Australia, and identifiable information about their health is collected in the GP's clinical information system. From the GP's system, the data is uploaded to the Australian government's My Health Record system, which is accessible by any registered healthcare provider who is caring for the patient. The person receiving care is referred to a specialist clinic and undergoes surgery in a public hospital. In each of these locations, the person's health data is entered into local medical record systems and uploaded to the My Health Record system. The person's health information is thus held in systems that are regulated under both state and federal legal jurisdictions in Australia, by three different principal Acts (see Table 1).

A data breach occurs. This could be a phishing attack where a hacker gains unauthorised access to a system, a fax mistakenly sent to a wrong number, or it could be that someone at one of the clinics recognises the patient from a social context and accesses their record for interest, using login information that is kept on a sticky note next to the computer screen. Whether the person whose health data was accessed or disclosed inappropriately must be notified of this event depends first on which medical record system is involved. Then, if it is a system subject to the *Privacy Act*, notification turns on whether the threshold requirements (eg likelihood of serious harm) have been met. If the data breach occurred in the public hospital, there is no requirement that the person be notified about it. This

59 'Guide to Mandatory Data Breach Notification in the My Health Record System', *Office of the Australian Information Commissioner* (Web Page, 6 October 2017) <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-mandatory-data-breach-notification-in-the-my-health-record-system>.

60 Ibid.

inconsistency of experience must be nonsensical to consumers for whom the jurisdictional boundaries are largely invisible. Further, there is evidence that people in Australia expect to be told when their data is subject to a breach,[61] and this expectation is not met by state-based public health services.

In addition to impacting on the consumer experience, another important consequence of fragmentation is unnecessary administrative complexity for healthcare providers and organisations, who must determine whether the different thresholds for notification under the *Privacy Act* compared with the *My Health Records Act* have been met, as well as which agency has to be advised. It is not unusual for specialists to practise in both public hospitals and private clinics. The use of the My Health Record system is increasing across all clinical settings.[62] Each of these contexts demands different actions in response to a health data breach. There does not appear to be evidence available on how well healthcare providers understand their responsibilities for breach notification to individuals and reporting to regulators under the different schemes.

Finally, a complete picture of health-related data security in Australia is lacking, in part because of this fragmentation of notification schemes, coupled with the divergence in agency practices for publishing summary data about breach notifications over a given period (noted earlier). The different definitions of a notifiable data breach that are given in the *Privacy Act* and the *My Health Records Act* are likely to result in heterogenous data about the nature and extent of data breaches in healthcare, which are difficult to evaluate reliably. To the extent that crafting an effective solution to data breaches relies upon clear and dependable information about the nature and extent of the problem, the lack of a comprehensive and consistent approach to notification and reporting may undermine the quality of the solution being designed.

Overall, this poor integration constitutes a failure of regulation to respond to the significant challenge of health data breaches in Australia. In the next section, I present a detailed analysis of what the mandatory data breach notification laws in Australia aim to achieve, and how relevant these goals are for breaches of health data specifically. I posit that a number of adjustments are needed to the design and operation of these schemes in order to enhance the capacity of data breach notification to benefit healthcare recipients.

61 Jayne Van Souwe et al, Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2017* (Report, May 2017) 16 <https://www.oaic.gov.au/engage-with-us/research/2017-australian-community-attitudes-to-privacy-survey/report>.

62 *Statistics and Insights: July 2022* (n 11) 2.

IV WHY NOTIFY? ANALYSING DATA BREACH NOTIFICATION PURPOSES IN THE AUSTRALIAN CONTEXT

Notifying people whose data have been subject to a breach has inherent appeal. It seems both fair and empowering to data subjects. As a legally enforceable instrument in the data privacy toolkit, with substantial penalties available to regulators for non-compliance, data breach notification is also worthy of closer examination in terms of its aims and effects. In the following analysis I argue that Australian breach notification schemes are not, at present, functioning optimally in respect of health data breaches and their consequences for consumers.

To investigate this issue, I surveyed international literature on data breach notification to develop a conceptual map or typology of purposes. This is presented in Table 2, with the purposes of breach notification given in no particular order. They include individual harm mitigation, data security improvements, transparency, and system-wide learnings. This survey brings to the surface the multiple and sometimes unrealistic goals of mandatory notification schemes in the event of a data breach.

Scholars have tackled this issue before. Schafer, in a 2017 paper, sets out an analysis focusing on the objectives of individual compensation and 'self-help' harm mitigation, transparency, system-wide learnings and pre-emptive data security improvements.[63] Daly and Burdon conceptualised this type of regulatory response in two ways: the US model that is generally angled towards the avoidance or mitigation of cybercrime,[64] compared with the European Union's approach in the *GDPR* that takes a more rights-based approach in the context of an overarching privacy regime.[65] The analysis presented in Table 2 updates and expands upon this previous work, adding three new categories (identified from the literature) to the framework developed by Schafer: punishment of the data controller, reduction in the overall cost of doing business, and overcoming the lack of market incentives.

Table 2. Why Notify? An Updated Typology of Purposes for Data Breach Notification

1.	Harm mitigation and compensation (at data subject level)	*People whose data have been inappropriately accessed, disclosed or lost are at heightened risk of harm (including identity theft, fraud, public embarrassment, psychological harm, stigma). Awareness of a data breach will motivate individuals to act so as to mitigate their harm, for example by taking steps to secure their identity, monitoring their assets against fraud, and seeking financial compensation for breach of privacy.*

63 Burkhard Schafer, 'Speaking Truth to/as Victims: A Jurisprudential Analysis of Data Breach Notification Laws' in Mariarosaria Taddeo and Luciano Floridi (eds), *The Responsibilities of Online Service Providers* (Springer International Publishing, 2017) 79 <https://doi.org/10.1007/978-3-319-47852-4_5>.

64 Mark Burdon, 'Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws' (2010) 27(1) *Santa Clara Computer and High Technology Law Journal* 63, 86.

65 Daly (n 28) 494.

2.	Motivating pre-emptive data security improvements (at data controller level)	*The fear of being subject to a data breach necessitating notification to affected individuals, leading to shareholder disapproval and public notoriety, will motivate data controllers to pre-emptively improve security practices in their individual organisations.*
3.	Transparency	*People have a right to know when their data are accessed inappropriately or are lost. Data controllers have a responsibility to disclose data breaches. Doing so will ensure accountability to data subjects and promote the public interest. Transparency is conceptualised both as a 'self-evident good',*[66] *promoting a healthy information environment,*[67] *but also a springboard to other purposes: pre-emptive improvements and system-wide learnings. Further, it supports informed consumer choice by reducing information asymmetry.*[68]
4.	Overcoming the lack of market incentives for notification	*Because the market punishes entities that incur a data breach, they are unlikely to notify data subjects of their own volition or even with encouragement but must be regulated to do so. This purpose assumes that notification can achieve other goals, such as individual harm mitigation and transparency.*
5.	Punishment of data controller	*The breach notification requirement indirectly punishes data controllers subject to a breach — who, it must be remembered, may themselves be victims.*[69] *First, the act of breach notification imposes a cost, often significant, upon the notifying entity, which may be increased through post-notification measures such as activities involved in securing or monitoring accounts. It also exposes them to the risks of reputational damage, adverse media attention, market chastisement in the form of reduced sales and plunging share price,*[70] *and fewer customers. Sunstein notes that 'the punishment may be mild, optimal, or excessive and alarmist, and it can be hard to predict in advance'.*[71]
6.	Reduced identity fraud reduces overall cost of doing business	*If individuals who are notified of data breaches take steps to secure their identity, or security practices are enhanced pre-emptively so that data breaches are reduced, identity fraud will be reduced overall. This decreases overall costs for organisations.*[72]

66 Amitai Etzioni, 'Is Transparency the Best Disinfectant?' (2010) 18(4) *Journal of Political Philosophy* 389, 389.

67 Schafer (n 63) 90.

68 Juhee Kwon and M Eric Johnson, 'The Market Effect of Healthcare Security: Do Patients Care about Data Breaches?' (Conference Paper, The Workshop on the Economics of Information Security, 2015) 3–4.

69 Schafer (n 63) 92–3.

70 Sanjay Goel and Hany A Shawky, 'The Impact of Federal and State Notification Laws on Security Breach Announcements' (2014) 34 *Communications of the Association for Information Systems* 37, 46 <https://aisel.aisnet.org/cais/vol34/iss1/3>.

71 Cass R Sunstein, 'Informational Regulation and Informational Standing: *Akins* and Beyond' (1999) 147(3) *University of Pennsylvania Law Review* 613, 630.

72 Michael Turner, Information Policy Institute, *Towards a Rational Personal Data Breach Notification Regime* (Report, June 2006) 20–1 <https://www.perc.net/wp-content/uploads/2013/09/data_breach.pdf>.

7.	System-wide learnings	*Related to the 'transparency' goal, data breach notification may also yield new insights across whole industry sectors or geographic areas about the nature of the problem and which protective measures are effective,*[73] *which can in turn support system-wide improvements in security awareness and practices, and harm mitigation tools.*

A *Applying the Typology to Australian Data Breach Notification*

To examine the Australian approach to data breach notification schemes in greater depth, in order to better determine their fitness for purpose — especially for health data — I conducted a thematic analysis of Australian source materials pertinent to the domestic legislative schemes. I first gathered documents related to the introduction of mandatory data breach notification in the *Privacy Act* and the *My Health Records Act*. These included explanatory memoranda and Second Reading Speeches, as well as government and ALRC reports and consultative documents that preceded the introduction of the new legislation. The documents analysed are listed in Appendix 1. Any reference to the purpose of breach notification laws within these documents was coded against the above typology using NVivo software,[74] employing a deductive approach.

Table 3. Breach Notification Goals: An Analysis of Australian Legislative Materials

1.	Individual harm mitigation and compensation	24 references in 9 documents
2.	Motivating pre-emptive data security improvements (at data controller level)	10 references in 6 documents
3.	Transparency	12 references in 5 documents
4.	Overcoming the lack of market incentives for notification	6 references in 3 documents
5.	Punishment of data controller	2 references in 1 document
6.	System-wide learnings	2 references in 2 documents
7.	Reduced identity fraud reduces overall cost of doing business	1 reference in 1 document

The thematic analysis, summarised in Table 3, bears out the updated typology of mandatory data breach notification purposes described earlier. It also demonstrates that the Australian breach notification schemes are dominated by the following three stated purposes:

1. Individual harm mitigation by data subjects;
2. Pre-emptive improvement of data security measures by organisations; and

73 *OECD Privacy Framework* (n 19) 26.

74 QSR International, 'Get Started with NVIVO Today', *NVIVO* (Web Page) <https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home>.

3. Transparency (broadly defined).

Because of their dominance, these three concepts will be interrogated further in the following section, particularly in relation to health data breaches, to consider whether they are appropriate and attainable goals to be pursued through the mechanism of data breach notification laws.

V REFLECTIONS ON THE PRINCIPAL GOALS OF AUSTRALIAN DATA BREACH NOTIFICATION SCHEMES

A *Individual Harm Mitigation and Compensation*

1 *Data Breaches Not Limited to Health*

Individual harm mitigation is by far the most commonly stated goal of data breach notification schemes in Australia. This activity assumes the existence of a rational individual data subject who has sufficient resources to undertake the mitigation activities that have been recommended. These activities may include such things as: changing passwords for email, bank and other online accounts; ensuring that anti-virus software is installed and up-to-date; being more cautious than usual in disclosing personal information over the phone or of opening unsolicited emails; reviewing bank statements or a personal credit report; obtaining credit and identity monitoring services and identity insurance; and taking steps to alleviate personal distress (such as contacting a support service or seeking advice from a doctor). As Sunstein has indicated, the expectation that breach notification will cause a person to take steps to mitigate their potential harm ignores the possibility of notification fatigue ('information overload'), 'optimistic bias' (the belief that one is immune to risks that are significant for others), and the differential response by those who are less well equipped in terms of knowledge, motivation and resources, to act upon the notification.[75] It assumes that 'those who receive the information released by producers or public officials can properly process it and that their conclusions will lead them to reasonable action'.[76] This concern about the expectation or likelihood of a causative harm mitigation effect has been borne out in various studies, with data from the US repeatedly indicating that fewer than half of consumers notified of the risk or actuality of identity theft after a data breach took any action.[77] At the date of writing, there do not appear to be any empirical data in Australia about how affected people respond to data breach notification.

75 Sunstein (n 71) 627–8.

76 Etzioni (n 66) 398.

77 Sasha Romanosky, Rahul Telang and Alessandro Acquisti, 'Do Data Breach Disclosure Laws Reduce Identity Theft?' (2011) 30(2) *Journal of Policy Analysis and Management* 256, 281.