AUSTRALIA WOULD BENEFIT FROM US-STYLE HEALTH INFORMATION SECURITY REGULATION

JADE M KELLY*

ABSTRACT

Since 2018, the Australian healthcare industry has reported the highest incidence of data breaches of all industries reporting under the Notifiable Data Breaches ('NDB') scheme. This paper examines and compares Australia's health information security and breach notification laws to equivalent United States ('US') rules under the *Health Insurance Portability and Accountability Act* ('*HIPAA*') of 1996. Unlike the US, Australia does not have mandatory security standards for the protection of electronic health information, and the NDB scheme does not require that breach notifications be issued for all incidents in which the privacy or security of health information is compromised. Consequently, there is less emphasis on security in the Australian healthcare industry compared to the US, which has contributed to the industry's high incidence of data breaches. To strengthen the Australian healthcare industry's culture of security, this paper recommends modifications to the NDB scheme and the introduction of health information security regulations like the *HIPAA* Security Rule.

I INTRODUCTION

The Australian government is closely monitoring the state of Australia's information security. Last year, the Morrison Government announced amendments to bolster the enforcement of the *Privacy Act 1988* (Cth) ('*Privacy Act*'). This year, the government issued its 2020 Cyber Security Strategy.[1] In preparing this strategy, the government considered submissions that the healthcare industry needs data security regulations.[2] Such arguments are warranted because health information is heavily digitised and a prime target for cyber-attacks.[3] Since 2018, the healthcare industry has reported the highest incidence of data breaches of all industries reporting under the Notifiable Data Breaches ('NDB') scheme. According to the government, these breaches stem from insufficient security measures and a lack of training within the healthcare industry.[4] Presently, neither the *Privacy Act* nor its regulations contain any specific security requirements that effectively enforce the protection of health information.

This paper argues that Australia should seek to mitigate healthcare breaches by adopting health information security regulations and by making modifications to the NDB scheme that

* Jade M Kelly, LLM, LLB is a PhD candidate at the Australian Centre for Health Law Research, Queensland University of Technology. She previously practised health law in California, and her area of focus is health information privacy and security.

[1] Department of Home Affairs, *Australia's Cyber Security Strategy* (August 2020).

[2] Commonwealth Scientific and Industrial Research Organisation (CSIRO), Submission No 87 to Department of Home Affairs, *Australia's 2020 Cyber Security Strategy* (November 2019) 4–7; Monash University, Submission No 172 to Department of Home Affairs, *Australia's 2020 Cyber Security Strategy* (November 2019) 1.

[3] Threat Resistance Unit, Armor, *The Armor 2019 Black Market Report: A Look Inside the Dark Web* (September 2019) 38 <https://cdn.armor.com/app/uploads/2018/10/2019-Q3-Report-BlackMarket-SinglePages-1.pdf>.

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

draw upon the United States ('US') regulations. The US *Health Insurance Portability and Accountability Act* ('*HIPAA*')[5] of 1996 and its implementing regulations apply to most US healthcare providers, health plans, healthcare clearinghouses and their business associates. These entities must implement security standards and associated specifications to ensure the privacy, integrity and availability of health information within their control.[6] These entities must also report breaches that compromise health information, even if there is no serious harm to the affected individuals.[7] Breaches caused by violations of HIPAA are subject to significant enforcement action by US regulators.[8]

Part II of this paper highlights the prevalence of cyber-attacks and the importance of security within the healthcare industry; Part III examines and compares health information security requirements in Australia and the US; Part IV compares the NDB scheme with breach notification provisions under *HIPAA*; and Part V argues that the culture of security within Australian healthcare organisations needs to be strengthened. To improve the industry's culture of security and thus minimise healthcare breaches, this paper recommends that flexible health information security regulations be introduced based on *HIPAA*'s security requirements. Finally, this paper recommends that the NDB scheme be modified to bolster the enforcement of any such security regulations.

II Security is Fundamental to Maintaining the Privacy of Health Information

According to AustCyber, a government-funded science body, as a powerful player in the global economy, Australia is increasingly targeted by cybercriminals. However, unlike the US and Europe, Australia has been slow to take cybersecurity seriously.[9] The Australian health sector is particularly vulnerable to targeted cyber-attacks because digital health records contain a wealth of personal information, including full names, addresses, dates of birth, tax identification numbers, health insurance identifiers, driver license numbers, emergency contacts and payment card details.[10] On the dark web, for example, cybercriminals pay up to AUD1,000 per digital

[5] *Health Insurance Portability and Accountability Act of 1996*, 42 USC §§ 1320d–1320d-9 (2010).
[6] Pursuant to 45 CFR §§ 164.302–164.318 (2013) ('the *HIPAA Security Rule*').
[7] Pursuant to the *HIPAA* Breach Notification Rule. Ibid §§ 164.400–164.414.
[8] Ibid §§ 160.312, 160.402.
[9] David Wroe, 'Australia an Easy "Testing Ground" for Hackers: Cyber Industry Chief', *The Sydney Morning Herald* (March 2019) <https://www.smh.com.au/politics/federal/australia-an-easy-testing-ground-for-hackers-cyber-industry-chief-20190308-p512v0.html>.
[10] Threat Resistance Unit (n 3) 38.

health record, as they can use the information therein for credit card fraud, identity theft and other nefarious purposes.[11] Notably, the affected healthcare organisation can incur AUD400 in notification and other costs for each health record breached.[12]

Since the NDB scheme was introduced in 2018, the Australian private health sector has reported more data breaches to the Office of the Australian Information Commissioner ('OAIC') than any other industry. Initially, most of these breaches resulted from human error.[13] However, over the past year there has been a marked increase in the number of breaches caused by cyber incidents (i.e., malicious or criminal cyber-attacks).[14] From 1 July to 31 December 2019, 54 per cent of private health sector data breaches were the result of cyber incidents.[15]

Cybercriminals have only recently focused on the Australian healthcare industry. Conversely, the US healthcare industry has long been plagued by cyber-attacks. In the US, *HIPAA* breaches caused by hacking and other information technology ('IT') incidents are reportable to the Department of Health and Human Services' Office for Civil Rights ('OCR'). In relation to the breaches reported to OCR in 2019, 59 per cent were caused by hacking or IT incidents; a figure up from 34 per cent in 2016.[16] The increased proportion of breaches caused by hacking or IT incidents correlates with the dramatic rise in cyber-attacks on US healthcare entities over the past few years. A similar proportion of Australian and US healthcare breaches are caused by cyber incidents; however, Australia has a high breach rate compared to the US. As discussed further below in Part V, this is because the US healthcare industry has cultivated a strong culture of security to mitigate breaches caused by cyber-attacks.[17] Indeed, the proportion

[11] Beverly Head, 'Hackers target Australian health sector, selling records for A$1,000' (7 October 2015) *Computer Weekly* <https://www.computerweekly.com/news/4500254986/Hackers-target-Australian-health-sector-selling-records-for-A1000>; Andrew Steger, 'What Happens to Stolen Healthcare Data?' (30 October 2019) *Health Tech Magazine* <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon>.

[12] Honan, 'Health care industry hit by more cyber breaches than any other sector in Australia' (22 July 2019) <https://honan.com.au/news/health-care-industry-hit-by-more-cyber-breaches-than-any-other-sector-in-australia/>.

[13] Office of the Australian Information Commissioner (n 4) 5, 13.

[14] Australian Associated Press, 'Systems shut down in Victorian hospitals after suspected cyber attack', *The Guardian* (1 October 2019) <https://www.theguardian.com/australia-news/2019/oct/01/systems-shut-down-in-victorian-hospitals-after-suspected-cyber-attack>; Lucy Cormack, 'Australian business 'completely unprepared' for cyber hacks, up 700%', *The Sydney Morning Herald* (1 August 2019) <https://www.smh.com.au/national/nsw/australian-business-completely-unprepared-for-cyber-hacks-up-700-percent-20190731-p52cm8.html>.

[15] Office of the Australian Information Commissioner, 'Notifiable Data Breaches Report: July–December 2019' (Report, 28 February 2020) 18 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019>.

[16] HIPAA Journal, 'Healthcare Cybersecurity', *2019 Healthcare Data Breach Report* (Web Page, 13 February 2020) <https://www.hipaajournal.com/2019-healthcare-data-breach-report/>; HIPAA Journal, 'Healthcare Cybersecurity' *Largest Healthcare Data Breaches of 2016* (Web Page, 4 January 2017) <https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/>. These statistics are only for large reported data breaches that affect at least 500 individuals. The OCR does not publish data for smaller reported breaches.

[17] Healthcare Information and Management Systems Society, *2019 HIMSS Cybersecurity Survey* (Final Report, 2019) 3–7 <https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf>.

of *HIPAA* breaches caused by hacking and IT incidents over the past few years may partly reflect improved monitoring and detection by US healthcare organisations.[18]

The prevalence of healthcare breaches caused by cyber incidents underscores the importance of implementing robust security measures to protect health information; security is critical to maintaining privacy.[19] Many breaches may have been prevented if the subject organisations had placed greater emphasis on information security. It is well established within the information security industry that performing a comprehensive risk assessment is fundamental to identifying security issues. In turn, a risk management plan should be adopted that implements reasonable security safeguards to minimise identified risks. This is an ongoing process that requires continual monitoring, frequent reassessments and updates to identify and manage new and existing risks.[20] Additionally, providing staff members with adequate training in relation to security policies and procedures is critical for compliance.[21] As discussed further below, the aforementioned information security practices are key requirements under *HIPAA*. However, no such security provisions are contained in the *Privacy Act* and the regulatory guidelines only address these practices at a superficial level.

III Unlike US Regulations, Australian Health Information Security Requirements are not Comprehensive

A *Australian Legislation and Guidance Materials*

Australia has strict federal, state and territory privacy laws for personal information, including health information. However, it does not have detailed laws or regulations that mandate specific security standards for the protection of health information or other personal information. Rather,

[18] HIPAA Journal, 'Healthcare Cybersecurity' *Healthcare Data Breach Statistics* (Web Page) <https://www.hipaajournal.com/healthcare-data-breach-statistics/>.
[19] US Department of Health and Human Services Office for Civil Rights, *Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2015, 2016, and 2017* (22 February 2019) 24–6 <https://www.hhs.gov/sites/default/files/breach-report-to-congress-2015-2016-2017.pdf>; Office of the Australian Information Commissioner (n 4) 13.
[20] Jean Josephine Siganto, 'Transparent, Balanced and Vigorous: The Exercise of the Australian Privacy Commissioner's Powers in Relation to National Privacy Principle 4' (PhD Thesis, Queensland University of Technology, 2015) 82–8; Kim Offner et al, 'Towards Understanding Cybersecurity Capability in Australian Healthcare Organisations: A Systematic Review of Recent Trends, Threats and Mitigation' (2020) 35(4) *Intelligence and National Security* 556, 567–8.
[21] Heather Landi, 'Former OCR Advisor on HIPAA Compliance and Data Breaches: "This is a Management Problem, Not a User Problem"', *Healthcare Innovation Group* (13 April 2017) <https://www.hcinnovationgroup.com/cybersecurity/article/13028399/former-ocr-advisor-on-hipaa-compliance-and-data-breaches-this-is-a-management-problem-not-a-user-problem>; Office of the Australian Information Commissioner (n 4) 13.

Australian regulators provide the healthcare industry with general guidance on information security measures that references US guidelines and standards.

1 *Privacy Act 1988 (Cth)*

Pursuant to the *Privacy Act*, Australia aims to maintain the privacy of health information and other personal information about identifiable or reasonably identifiable individuals. The *Privacy Act* applies to federal government agencies, organisations with an annual turnover of more than AUD3 million, all private sector health providers and certain other entities that handle personal information.[22] Under the *Privacy Act*, health information qualifies as 'sensitive information', which is a subset of personal information that is afforded special protections.[23] The *Privacy Act* has specific provisions that govern the collection, use and disclosure of health information.[24] It also contains the Australian Privacy Principles ('APPs') that outline requirements related to the management, collection, storage, use, disclosure, correction, integrity of and access to personal information.[25]

APP 11 relates to the security of personal information and states that an entity that holds personal information must take 'reasonable steps' under the circumstances to protect the personal information from unauthorised access, modification, disclosure, misuse, interference or loss.[26] APP 11 further mandates the destruction or deidentification of personal information when it is no longer needed for its permissible purpose and retention is not otherwise required.[27] An entity must also take reasonable steps in the circumstances to implement procedures, systems and practices to ensure its compliance with APP 11 and the other APPs.[28]

APP 11 does not detail the reasonable steps that entities should take to protect or secure health information. However, the OAIC's guidance on APP 11 notes that the 'reasonable steps' that need to be taken will depend on an entity's circumstances. It is critical that the entity identify the nature and scope of the personal information held and the consequences to the individual if such information is subject to a breach. An entity should consider the practical implications of each possible security measure given its size and resources. An entity should also consider

[22] *Privacy Act 1988* (Cth) s 6C. The *Privacy Act* does not govern state and territory government agencies. Each state or territory has separate privacy laws for its public entities.
[23] Ibid s 6(1) (definition of 'sensitive information').
[24] Ibid s 16B.
[25] Ibid sch 1.
[26] Ibid sch 1, APP 11.1.
[27] Ibid sch 1, APP 11.2.
[28] Ibid sch 1, APP 1.2.

whether the measure itself is invasive of privacy. According to the OAIC, reasonable steps should include, as relevant: internal practices, procedures and systems; information and communication technology ('ICT') security; access security; physical security; governance, culture and training; third-party providers; standards; destruction and de-identification; and data breaches.[29]

A few Australian states have health record privacy legislation for the private sector that applies in conjunction with the *Privacy Act*.[30] Like APP 11, this state legislation generally requires the protection of health information using safeguards reasonable under the circumstances, but does not specify the reasonable security measures that need to be implemented.[31]

2 *My Health Record and National Identifiers*

There are also data protection obligations for Australia's national electronic health record system, My Health Record, and the Individual Healthcare Identifier ('IHI') linked to each individual's My Health Record.[32] If the My Health Record System Operator is satisfied that a healthcare provider may compromise the security or integrity of the My Health Record system, it can deny access to a My Health Record.[33] Access can be suspended if there is a risk to the security, integrity or operation of the My Health Record system.[34] Similarly, healthcare providers and other entities authorised to handle IHIs must protect each IHI from unauthorised access, modification, disclosure, misuse or loss.[35]

3 *Health Information Security Guidance*

The Australian privacy laws and their associated regulations do not contain any specifications about securing health information. However, the OAIC, the Australian Digital Health Agency ('ADHA') and the Australian Cyber Security Centre have published guidance materials.[36] The

[29] Office of the Australian Information Commissioner, 'Australian Privacy Principles Guidelines', *Chapter 11: Australian Privacy Principle 11—Security of personal information* (Web Page, 22 July 2019) 4 <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/>.
[30] *Health Records and Information Privacy Act 2002 No 71* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).
[31] *Health Records and Information Privacy Act 2002 No 71* (NSW) Sch 1, HPP 5; *Health Records Act 2001* (Vic) Sch 1, HPP 4; *Health Records (Privacy and Access) Act 1997* (ACT) Sch 1, PP 4.1.
[32] An IHI is used to verify the individual's identity, and accurately link his or her health information with the correct My Health Record. *Healthcare Identifiers Act 2010* (Cth) s 3.
[33] *My Health Records Act 2012* (Cth) s 44(2).
[34] *My Health Records Rule 2016* (Cth) s 17.
[35] *Healthcare Identifiers Act 2010* (Cth) s 27(a).
[36] The Royal Australian College of General Practitioners has also published its own security guidance available at <https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Security/Information-Security-in-General-Practice.pdf>.

ADHA guidance materials include an information security guide for small healthcare providers. The guide contains security questions on various topics, from common threats and security awareness to device security and backups. Notably, the materials recommend a small business information security guide published by the US National Institute of Standards and Technology ('NIST') and cybersecurity tips for healthcare from the US Department of Health and Human Services ('HHS').[37] The OAIC's guidance materials reference some additional resources, including the National eHealth Security and Access Framework ('NESAF').[38] All of these guidance materials are high-level and do not provide detailed information on the security safeguards and processes necessary for compliance with APP 11.[39]

B *US Legislation, Regulations and Guidance*

Like Australia, the US has strict federal and state laws for the privacy of health information, including a federal law known as *HIPAA*.[40] Unlike Australia, US regulations (enacted under *HIPAA*) set specific security standards and implementation specifications for the protection of health information.[41] For example, in the US, most healthcare providers are required to perform a security risk analysis, implement a risk management plan and provide information security training to their workforce.[42] Additionally, US regulators provide the healthcare industry with specific guidance regarding compliance with these health information security regulations. As discussed in this part, aggressive enforcement action is taken when breaches result from a failure to comply with the security requirements.

1 *HIPAA*

HIPAA governs protected health information ('PHI'), including health records and healthcare billing records. PHI is broadly defined to include any individually identifiable health information

[37] Australian Digital Health Agency, *Information Security Guide for Small Healthcare Businesses* (December 2018) <https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/information-security-guide-for-small-healthcare-businesses/HD127%20Information%20Security%20Guide%20for%20small%20healthcare%20businesses%20(co-branded%20with%20Stay%20Smart%20Online)%20Online%20Version.pdf>.

[38] Office of the Australian Information Commissioner, *Guide to securing personal information* (5 June 2018) <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/>. Similar to NIST, NESAF provides guides, tools and standards for Australian healthcare organisations to use when building security systems. Australian Digital Health Agency, *National eHealth Security and Access Framework v3.1* <https://developer.digitalhealth.gov.au/specifications/ehealth-foundations/ep-1005-2012>.

[39] See Siganto (n 20) 174–76.

[40] *Health Insurance Portability and Accountability Act of 1996*, 42 USC §§ 1320d–1320d-9 (2010).

[41] 45 CFR § 160.103 (2013) (definition of 'covered entity').

[42] Ibid §§ 164.302–164.318.

created, received, stored or transmitted in relation to the provision of healthcare, healthcare operations and payment for healthcare services.[43] The *HIPAA* regulations issued by the HHS[44] contain a Privacy Rule,[45] a Security Rule[46] and a Breach Notification Rule.[47] These rules apply to *HIPAA* 'covered entities' (i.e., health plans, healthcare clearinghouses and healthcare providers who engage in standard electronic transactions).[48]

The *HIPAA* rules apply to healthcare providers operated by US states, territories and local governments. Many of the rules also apply to a covered entity's third-party providers and other 'business associates', who create, receive, maintain or transmit PHI on behalf of a covered entity (or another business associate).[49] Additionally, a covered entity must enter into a 'business associate agreement' with each business associate to obtain satisfactory assurances that the business associate will safeguard the PHI and comply with certain *HIPAA* privacy, security and breach notification requirements.[50]

2 *The HIPAA Privacy Rule*

The *HIPAA* Privacy Rule governs the use and disclosure of PHI by covered entities and business associates (each of which is a *HIPAA* entity).[51] In relation to security, the Privacy Rule contains a general provision requiring each covered entity to protect PHI from unauthorised use or disclosure by implementing appropriate administrative, physical and technical safeguards.[52] This provision is comparable to APP 11 of the *Privacy Act*.

3 *The HIPAA Security Rule*

The *HIPAA* Security Rule goes further than the Privacy Rule, as it requires certain physical, administrative and technical safeguards be implemented to protect electronic PHI ('ePHI').[53] These safeguards are aimed at ensuring the confidentiality, availability and integrity of the ePHI

[43] Ibid § 160.103 (definition of 'protected health information').
[44] The regulations were issued pursuant to *HIPAA*, but subsequently modified pursuant to the *Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009* (enacted under Title XIII of *the American Recovery and Reinvestment Act of 2009*, Pub. L. No. 111-5, 123 Stat 115).
[45] 45 CFR §§ 164.500–164.534 (2013).
[46] Ibid §§ 164.302–164.318.
[47] Ibid §§ 164.400–164.414.
[48] Ibid § 160.103 (definition of 'covered entity'). These standards for electronic exchange of information for financial or administrative activities related to health care include payment and remittance advice, claims status, eligibility; coordination of benefits, claims and encounter information, enrolment and disenrollment, referrals and authorisations and premium payment (at §§ 162.100–162.1902).
[49] Ibid § 160.103 (definition of 'business associate').
[50] Ibid §§ 164.308(b), 164.314(a), 164.504(e).
[51] Ibid §§ 160.101–160.552, 164.102–164.534.
[52] Ibid § 164.530(c).
[53] Ibid §§ 164.302–164.318.

created, received, maintained and transmitted by each *HIPAA* entity. These safeguards further aim to protect ePHI from unauthorised use or disclosure and from threats or hazards to its security or integrity.[54]

(a) Administrative Safeguards

To comply with the Security Rule's administrative safeguards, each *HIPAA* entity must implement written policies and procedures to prevent, detect, contain and correct security issues. The *HIPAA* entity must conduct an accurate and thorough risk analysis and implement a risk management plan with sufficient measures to reduce identified risks and vulnerabilities. It must also implement a security awareness and training program for its workforce members. A sanctions policy is required to appropriately sanction workforce members who do not comply with security policies and procedures. Information system activity reviews must be conducted regularly to review information system records. Policies and procedures must ensure appropriate access to ePHI by workforce members and others. The HIPAA entity must also implement security incident procedures, a contingency plan, a data backup plan, a disaster recovery plan and an emergency mode operation plan.[55]

(b) Technical Safeguards

The Security Rule also mandates certain technical safeguards. Notably, each *HIPAA* entity must adopt procedures to authenticate identity before providing access to ePHI. There must be access controls for its electronic information systems, including unique user identification and emergency access procedures. Each *HIPAA* entity must also implement technical safeguards to protect against unauthorised access for ePHI in transit. Audit controls are required to record and examine activity in information systems with ePHI. There must be procedures to protect ePHI from improper destruction or alteration.[56] Additionally, the encryption of ePHI at rest and in transit have addressable implementation specifications; however, it is considered best practice to encrypt data in transit and at rest, as encrypted PHI is not subject to the *HIPAA* Breach Notification Rule.[57]

(c) Physical Safeguards

Complying with the rule's physical safeguards involves implementing facility access controls, measures for workstation use and security, and device and media controls. Most of the associated

[54] Ibid § 164.306(a).
[55] Ibid §§ 164.308(a)(1), (3)–(8).
[56] Ibid § 164.312.
[57] Ibid §§ 164.312(a)(2)(iv), (e)(2)(ii) (2013); at § 164.402 (definition of 'breach' and 'unsecured protected health information').

implementation specifications are addressable, except that the *HIPAA* entity must adopt procedures for disposal of ePHI and media re-use.[58]

(d) Flexibility

The Security Rule is flexible in that it allows a *HIPAA* entity to meet each administrative, technical and physical safeguard by using security measures appropriate to its organisation.[59] The *HIPAA* entity must comply with each security standard for all ePHI; however, each standard's implementation specifications are either required or addressable. If addressable, the *HIPAA* entity must assess whether the specification is reasonable and appropriate in the *HIPAA* entity's environment in conjunction with the likelihood that it will protect the ePHI. If reasonable and appropriate, the specification should be implemented. If not, written documentation must be provided explaining why the specification is not reasonable and appropriate, and an equivalent alternative measure should be adopted if reasonable and appropriate.[60] The *HIPAA* entity must document, routinely review and update its plans, policies and procedures for implementing and complying with these security standards.[61] Additionally, a security officer must be appointed to oversee such responsibilities.[62]

4 *Regulatory Guidance*

In the US, the HHS publishes security guidance for the healthcare industry. This guidance emanates from requirements under the *HIPAA* Security Rule.[63] Unlike Australian health information security guidance, the HHS' guidance tends to be more specific. Notably, it frequently cites NIST standards in its guidance materials and has published a 'crosswalk' that correlates the Security Rule requirements with the NIST Framework for Improving Critical Infrastructure Cybersecurity.[64] However, a *HIPAA* entity can opt to implement other security frameworks that meet the requirements of the Security Rule.

---

[58] Ibid § 164.310.
[59] Ibid § 164.306(b).
[60] Ibid § 164.306(c)–(d).
[61] Ibid § 164.316.
[62] Ibid § 164.308(a)(2). For more information on the Security Rule's standards and specifications, the matrix at the end of the Security Rule is useful; at §§ 164.302–164.318, Appendix A.
[63] 45 CFR §§ 164.302–164.318 (2013).
[64] US Department of Health & Human Services, *Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework* (Web Page, 23 February 2016) <https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html>.

IV AUSTRALIA'S NDB SCHEME IS NOT AS STRINGENT AS THE *HIPAA* BREACH NOTIFICATION RULE

A *Different Standards*

In Australia and the US, health information breaches resulting from inadequate security or otherwise must be reported to regulators and the affected individuals. The US has strict breach notification rules for compromised PHI that is not encrypted or otherwise secured. Under these rules, breaches are reportable regardless of whether or not the breach harms the individuals whose PHI has been compromised. The low threshold for breach notification provides extra incentive for *HIPAA* entities to adequately secure PHI in accordance with the Security Rule. It also means that the OCR can identify and take appropriate enforcement action in circumstances in which PHI has been compromised due to inadequate security safeguards. Conversely, Australia only requires breach notification if an affected individual is likely to suffer serious harm. The NDB scheme does not directly apply to an organisation's third-party providers. Further, state and territory healthcare providers are not subject to the scheme. This makes it challenging for the Australian government to identify and address compromises to health information caused by inadequate security measures.

B *US Breach Notification*

In the US, many breaches stem from non-compliance with the *HIPAA* Security Rule.[65] This emphasises the close nexus between failures to implement security measures and the resulting PHI breaches.[66] Such breaches are reportable pursuant to the *HIPAA* Breach Notification Rule.[67] Under this rule, a reportable breach is presumed if there is any unauthorised acquisition, access, use or disclosure of 'unsecured' PHI[68] that compromises the security or privacy of the PHI.[69] Interestingly, the Breach Notification Rule previously required a 'significant risk of financial, reputational, or other harm to an individual' for a *HIPAA* violation to amount to a reportable breach. The harm standard seeks to avoid causing notification fatigue and alarm to affected individuals in inconsequential situations. In 2013, the HHS removed the harm threshold

[65] US Department of Health and Human Services Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information* (Web page) <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>.
[66] Sara M Smyth, 'Does Australia Really Need Mandatory Data Breach Notification Laws: And If So, What Kind?' (2013) 22(2) *Journal of Law, Information and Science* 159.
[67] 45 CFR §§ 164.400–164.414 (2013).
[68] PHI is considered unsecured if it is not encrypted, destroyed or otherwise rendered unusable, unreadable, or indecipherable in accordance with the HHS' guidance: Ibid § 164.402 (definition of 'unsecured protected health information').
[69] Ibid § 164.402 (definition of 'breach').

because, contrary to the HHS' original intent, the threshold was often manipulated by covered entities to avoid issuing breach notifications.[70]

Under the current rule, a *HIPAA* entity can rebut the breach presumption by conducting a risk assessment that shows a low probability that the unsecured PHI was compromised. The risk assessment must consider: the nature and extent of the PHI (including any identifiers it contains); the unauthorised user or recipient; whether the PHI was acquired or viewed; and the extent to which risk to the PHI has been mitigated.[71] The covered entity is required to mitigate any known harmful effect resulting from a breach by the covered entity or its business associate.[72] There are also a few limited breach exceptions related to unintentional good faith acquisitions, inadvertent internal disclosures and circumstances in which the retention of the disclosed PHI would not reasonably be possible.

A business associate must notify the covered entity, and the covered entity must notify each affected individual of the breach no later than 60 days after its discovery.[73] The written notice must be in plain language and include, among other things, a description of the breach and any steps the covered entity has taken (and the individual can take) to protect the individual from harm resulting from the breach.[74] If more than 500 residents of a state or jurisdiction are affected by a breach, the covered entity must also notify the media.[75] In situations in which a breach affects 500 or more individuals, the covered entity must notify the OCR at the same time as it notifies the affected individuals.[76] Each breach affecting 500 or more individuals will be posted on the OCR's website, commonly referred to as the *HIPAA* 'wall of shame'.[77]

Aside from the Breach Notification Rule, anyone who believes a *HIPAA* entity has violated the *HIPAA* rules can file a complaint with the OCR for investigation and resolution.[78] The OCR also has the authority to audit *HIPAA* entities in relation to their compliance with the rules.[79] Non-compliance can be very costly; civil money penalties range from USD117 to

[70] 78 Fed Reg 5566, 5639-40, 5642 (25 January 2013).
[71] 45 CFR § 164.402 (2013) (definition of 'breach').
[72] Ibid § 164.530(f).
[73] Ibid §§ 164.404, 164.410.
[74] Ibid § 164.404.
[75] Ibid § 164.406.
[76] If less than 500 individuals are affected, the covered entity must include the breach in an annual breach log submitted to OCR within 60 days of 31 December each year: Ibid § 164.408.
[77] US Department of Health and Human Services Office for Civil Rights (n 65).
[78] 45 CFR § 160.306 (2013).
[79] Ibid § 160.308.

USD1,754,698 per violation, depending on the *HIPAA* entity's level of knowledge. Each of the four penalty tiers has an annual cap for identical violations.[80]

The financial and reputational consequences of a breach provide strong incentives for compliance.[81] When breaches result from *HIPAA* violations, the OCR routinely enters into resolution agreements, whereby the *HIPAA* entity must take corrective action and pay a settlement. These settlements are posted on the OCR's website. Typically, there are about 10 such settlements per year and an occasional civil money penalty. In 2016, settlements and civil money penalties totalled USD23.5 million, jumping to USD28.7 million in 2018.[82] In 2019, total settlements and penalties dropped to USD12.27 million, but most alleged violations involved non-compliance with the Security Rule.[83]

C *Australian Breach Notification*

Australia's NDB scheme is relatively new. Since 2018, healthcare providers and other entities required to protect personal information under APP 11 of the *Privacy Act* are required to report eligible breaches under the NDB scheme.[84] The NDB scheme does not apply to third-party providers unless they are otherwise subject to APP 11.[85] This differs to the notification requirements for business associates under the *HIPAA* Breach Notification Rule.

Unlike the *HIPAA* Breach Notification Rule, the NDB scheme has a risk of harm standard. An eligible breach only occurs when there is an unauthorised disclosure of, access to or a loss of personal information that is likely to result in a serious risk of harm to one or more affected individuals and such risk has not been prevented by remedial action.[86] Serious harm is not defined under the scheme, but may include serious financial, reputational, psychological, emotional or physical harm.[87] Within 30 days of discovering the incident, the entity must conduct a serious harm assessment. This assessment should consider the circumstances of the breach

[80] 84 Fed Reg 59549 (5 November 2019); 45 CFR § 160.404 (2016).
[81] Mary Butler, 'Is HIPAA Outdated? While Coverage Gaps and Growing Breaches Raise Industry Concern, Others Argue HIPAA is Still Effective' (2017) 88(4) *Journal of AHIMA* 14.
[82] US Department of Health and Human Services Office for Civil Rights, *OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement* (Web Page) <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/2018enforcement/index.html>.
[83] US Department of Health and Human Services Office for Civil Rights, *Resolution Agreements and Civil Money Penalties* (Web Page) <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html>.
[84] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).
[85] Ibid ss 26WJ, 26WK(4), 26WM; Office of the Australian Information Commissioner, *Data Breach Preparation and Response* (Report, 13 July 2019) 54 <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response>.
[86] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) ss 26WE(2), 26WF.
[87] Office of the Australian Information Commissioner (n 85) 33.

and the type and sensitivity of information breached. The assessment should also consider the security measures in place to protect the information and whether those measures have rendered the information unintelligible or meaningless. Further, the assessment should identify the recipients of the information and the nature of the harm caused by the incident.[88] If the entity has reasonable grounds to believe that an eligible data breach occurred, it must promptly notify the OAIC and each affected individual as soon as practicable.[89] If the entity merely 'suspects' that it experienced an eligible breach, it need only notify the OAIC.[90] Non-eligible breaches do not need to be reported.

The NDB scheme is inapplicable if a data breach is subject to breach notification under the My Health Record system.[91] A My Health Record breach refers to any circumstances that involve the actual or potential unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record or compromises to the integrity or security of the My Health Record system. Registered healthcare provider organisations, contracted service providers and other My Health Record users must report actual or potential breaches to the ADHA (the system operator) as soon as possible. The ADHA is responsible for notifying healthcare recipients who might be seriously affected. The entity must contain the breach as far as it is reasonably practicable to do so.[92]

Like *HIPAA*, an individual may file a complaint with the OAIC if they believe their privacy has been interfered with.[93] The OAIC also has authority to conduct privacy assessments of entities subject to the *Privacy Act*.[94] Entities that engage in a serious or repeated act or practise that interferes with an individual's privacy may be subject to a civil penalty of AUD420,000.[95] For a body corporate, the maximum penalty may be five times that amount.[96] Last year, the Morrison Government announced that it will be amending this maximum from AUD2.1 million to the greater of: AUD10 million; three times the value of the benefit obtained from any misuse of information; or 10 per cent of the company's annual domestic turnover. Amendments to the *Privacy Act* will also include new penalties for failure to cooperate with the OAIC to resolve

[88] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) s 26WG.
[89] Ibid s 26WK.
[90] Ibid ss 26WH, 26WL.
[91] Ibid s 26WD.
[92] *My Health Records Act 2012* (Cth) s 75.
[93] *Privacy Act 1988* (Cth) s 36.
[94] Ibid s 33C.
[95] Ibid ss 13G, 25; *Crimes Act 1914* (Cth) s 4AA.
[96] *Regulatory Powers (Standard Provisions) Act 2014* (Cth) s 82(5)(a).

breaches and additional options for the OAIC to ensure breaches are properly addressed and those directly affected are advised.[97]

V Need For Australian Health Information Security Regulations

A *Healthcare Data Breaches Are Relatively High in Australia Compared to the US*

It is difficult to compare Australian and US breach figures because the breach notification requirements and published data differ. However, as discussed in this part, the data shows that healthcare breach rates are relatively high in Australia compared to those in the US. In the US, hundreds of large *HIPAA* breaches (i.e., breaches that affect at least 500 individuals) are reported to the OCR each year. The data for small breaches (i.e., breaches that affect under 500 individuals) is not published by the OCR, but presumably these are in the thousands per annum. From 1 April 2018 to 31 December 2019, an average of 38 large *HIPAA* breaches were reported to the OCR each month.[98] For the same period, an average of 18 breaches were reported to the OAIC by the Australian private health sector each month.[99] Of the total breaches reported to the OAIC across all industry sectors, the vast majority affected fewer than 1,000 people. The OAIC speculates that this may be due to poor practises by individual employees as opposed to larger breaches caused by single system compromises.[100] It may also be because many large security incidents are not covered by the NDB scheme.

The monthly average number of healthcare breaches reported in the US is just over twice that in Australia. Even so, Australia's breach rate is comparatively high for a number of reasons. First, many Australian security incidents are not reportable because the NDB scheme has a

[97] Attorney-General and Minister for Communications and the Arts, 'Tougher Penalties to Keep Australians Safe Online' (Joint Media Release, 25 March 2019).
[98] US Department of Health and Human Services Office for Civil Rights (n 19).
[99] Office of the Australian Information Commissioner, *Notifiable Data Breaches Statistics Report: 1 April to 30 June 2018* (Report, 31 July 2018) 13 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2018>; Office of the Australian Information Commissioner, *Notifiable Data Breaches Statistics Report: 1 July to 30 September 2018* (Report, 30 October 2018) 13 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-july-to-30-september-2018>; Office of the Australian Information Commissioner, *Notifiable Data Breaches Statistics Report: 1 October to 31 December 2018* (Report, 7 February 2019) 13 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-october-to-31-december-2018>; Office of the Australian Information Commissioner, *Notifiable Data Breaches Statistics Report: 1 January to 31 March 2019* (Report, 13 May 2019) 13 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-quarterly-statistics-report-1-january-31-march-2019>; Office of the Australian Information Commissioner, *Notifiable Data Breaches Statistics Report: 1 April to 30 June 2019* (Report, 27 August 2019) 13 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2019>; Office of the Australian Information Commissioner (n 15) 5.
[100] Office of the Australian Information Commissioner (n 4) 14.

higher threshold for breach notification than *HIPAA*. Second, the Australian population is around 13 times smaller than the US population.[101] Third, many breaches may go undetected because Australia does not have mandatory security measures to detect unauthorised access to private health record systems. Finally, the NDB scheme does not apply to state- and territory-operated healthcare providers, including public hospitals, which account for two thirds of Australian hospital beds.[102] There are likely many more health information breaches occurring within state and territory health systems that are not reflected in the NDB figures.[103]

B *The US Healthcare Industry Has a Strong Culture of Security Due to the Enforcement of the HIPAA Security Rule*

The US healthcare industry has a stronger culture of security than the Australian healthcare industry. This is largely due to the regulatory guidance about and the strict enforcement of the *HIPAA* Security Rule. The Australian healthcare industry does not have the same culture of security. This is likely due to many factors, including budget restrictions, a shortage of cybersecurity professionals and a lack of cybersecurity awareness.[104] The key factor is undoubtedly the ambiguity surrounding compliance with APP 11. According to the OAIC, complying with APP 11 is critical to mitigating the risk of data breaches.[105] However, such compliance is nebulous because there is no specificity regarding the 'reasonable steps' required under APP 11. As a result, Australian healthcare organisations and cybersecurity vendors often turn to US health information security standards for guidance.[106] Indeed, even the OAIC and the ADHA recommend the application of HHS' cybersecurity guidance materials and the NIST framework, which is the same framework that HHS' frequently refers to in the *HIPAA* Security Rule guidance materials.

The Security Rule has been effective in helping *HIPAA* entities prioritise information privacy. A US *HIPAA* compliance survey conducted in 2019 by SAI Global[107] found that most respondents had implemented *HIPAA* compliance programs aimed at complying with the *HIPAA*'s privacy, security and breach notification requirements. Of the 352 *HIPAA* entities

[101] World Bank, *Population, Total* (2018) <https://data.worldbank.org/indicator/SP.POP.TOTL>.
[102] Australian Institute of Health and Welfare, *Hospital resources 2016–17: Australian hospital statistics* (Report, 27 June 2018) 98 <https://www.aihw.gov.au/reports/hospitals/ahs-2016-17-hospital-resources/contents/table-of-contents>.
[103] Megan Prictor, 'Patients and the Data Breach Notification Maze' *Pursuit* (Blog Post, 10 August 2018) <https://pursuit.unimelb.edu.au/articles/patients-and-the-data-breach-notification-maze>.
[104] Offner et al (n 20) 557, 571–2.
[105] Office of the Australian Information Commissioner (n 85) 8.
[106] See Stanfield IT, *Data Breaches in Australia* <https://www.stanfieldit.com/data-breaches-in-australia>.
[107] In partnership with Strategic Management Services, LLC.

surveyed, 70% had completed a risk assessment, 95% stated they conduct *HIPAA* training on an annual basis, 93% stated they had had adopted *HIPAA* policies and procedures, and close to 90% of respondents claimed that they were either somewhat, mostly or very prepared for a *HIPAA* audit or investigation.[108] The effectiveness of the *HIPAA* in improving security is also evident when examining breach figures applicable to business associates. In 2013, business associates became directly subject to the Security Rule, the Breach Notification Rule and certain other *HIPAA* requirements.[109] Yaraghi and Gopal found that the direct application of these rules to business associates significantly reduced the number of *HIPAA* breaches caused by business associates.[110]

Recently, Offner performed a comprehensive review of Australia's cybersecurity literature in the healthcare context. She found little to no literature on the importance of creating a culture of cybersecurity within Australian healthcare organisations. Offner concluded that Australian healthcare organisations need to mature their cybersecurity culture to protect against cyber-attacks.[111] This stance is supported by a 2018 report by the Health Informatics Society of Australia ('HISA'). Of the 157 healthcare organisations surveyed by the HISA, only 33% conducted an annual risk assessment. One third of respondents indicated that cybersecurity awareness and training was included in their organisation's policies and procedures, most individuals did not know if their organisation had a written cybersecurity procedure or guide, and less than half of the organisations had a designated officer responsible for cybersecurity within the organisation.[112]

The HISA and the SAI Global survey questions and respondents varied; however, the results of both surveys indicate that Australian healthcare organisations have lower levels of training and security awareness than US *HIPAA* entities. Nevertheless, it should be noted that the SAI Global survey results may not paint an entirely accurate picture of *HIPAA* compliance. Several years ago, the last round of desk audits by the OCR showed that compliance with the *HIPAA* rules was largely inadequate.[113] For example, the desk audits revealed that around 94 per

[108] SAI Global, *2019 HIPAA Compliance Survey Report* (Report, 11 September 2019) <https://www.saiglobal.com/hub/industrynews/the-current-state-of-hipaa-compliance-2019>.
[109] 78 Fed Reg 5566 (25 January 2013).
[110] Niam Yaraghi and Ram D Gopal, 'The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights From an Empirical Study' (2018) 96(1) *The Milbank Quarterly* 144.
[111] Offner et al (n 20) 568, 572–3.
[112] Health Informatics Society of Australia, *Cybersecurity Across the Australian Healthcare Sector—Final Report of a National Survey* (Report, June 2018) <https://www.hisa.org.au/wp-content/uploads/2018/07/HISA-Healthcare-Cybersecurity-Report_June-2018.pdf>.
[113] The OCR reportedly has no plans at this stage to perform any additional audit rounds but continues its aggressive enforcement of the *HIPAA* with an emphasis on the Security Rule: Marianne McGee, '"No Slowdown" for HIPAA

cent of auditees failed to demonstrate appropriate risk management plans in compliance with the Security Rule.[114] That said, since 2016, US healthcare organisations have placed greater emphasis on the Security Rule due to a dramatic increase in cyber-attacks, hefty settlements with the OCR for alleged security violations and the fear of being audited.[115] Even with increased compliance, diligent *HIPAA* entities continue to experience breaches resulting from security issues.[116] HHS itself has significant weaknesses in its information security program.[117] It is impossible to completely eliminate health information privacy breaches; however, an effective health information security program would mitigate the risk of such breaches.

C *The Australian Healthcare Industry Needs Information Security Regulation*

The OAIC's 2019 annual breach report specifically identified the 'need for strong privacy governance in the health sector that includes robust and regular employee training and technological solutions to assist employees'.[118] To date, the OAIC has provided minimal guidance and enforcement action regarding the security principles contained in APP 11.[119] This has contributed to the healthcare industry having more breaches than any other single industry in Australia. The OAIC may now be better positioned to address the healthcare industry's cybersecurity issues, as it has received increased funding from the Morrison Government.[120] Added impetus may also come from the government's 2020 Cyber Security Strategy.

In preparing the 2020 Cyber Security Strategy, the government considered stakeholders' submissions as to why regulatory change is necessary.[121] For example, it considered the CSIRO's submission that security regulations should be sector specific, and that security regulations are particularly needed in the health and medical products sector.[122] Interestingly, one stakeholder contended that data encryption should be mandatory for the health sector by referencing the US

Enforcement, but Audits Ending' *Information Security Media Group* (Blog Post, 6 March 2018) <https://www.bankinfosecurity.com/no-slowdown-for-hipaa-enforcement-but-audits-ending-a-10701>.

[114] Linda Saches, 'Update on Audits of Entity Compliance with the *HIPAA* Rules' (Conference Paper, Conference on Safeguarding Health Information: Building Assurance through *HIPAA* Security, 6 September 2017) <https://cynergistek.com/wp-content/uploads/2017/09/OCR-CE-Desk-Audit-Results-09_17-.pdf>.

[115] See, eg, Butler (n 81); SAI Global (n 108); Healthcare Information and Management Systems Society (n 17) 8–13.

[116] HIPAA Journal, *Healthcare Associations Request Safe Harbor for Entities that Have Followed Cybersecurity Best Practices* (28 February 2019) <https://www.hipaaguide.net/healthcare-associations-request-safe-harbor-for-breached-healthcare-providers-that-followed-cybersecurity-best-practices>.

[117] HIPAA Journal, *OIG Gives HHS Information Security Program Rating of 'Not Effective'* (2 May 2019) <https://www.hipaajournal.com/oig-gives-hhs-information-security-program-rating-of-not-effective>.

[118] Office of the Australian Information Commissioner (n 4) 13.

[119] See Siganto (n 20) 327-335.

[120] Attorney-General and Minister for Communications and the Arts (n 97).

[121] Department of Home Affairs (n 1) 15.

[122] CSIRO (n 2) 4, 7.

encryption standard under *HIPAA*.[123] Even so, the 2020 Cyber Security Strategy does not specifically address cybersecurity reform for the health sector. However, it does identify the need for legislative change to 'clarify cyber security obligations for Australian businesses'.[124] This legislative change should include health information security regulations that address cybersecurity issues unique to the health sector. As discussed above, health information is extremely sensitive and valuable and thus is increasingly being subject to cyber-attacks. The interoperability of different healthcare networks, including My Health Record, raises challenging security issues. Secure network integration with medical and other internet-connected devices involved in the delivery of healthcare is also critical. Security regulations for the health sector must also ensure the availability and integrity of health information for patient care purposes.[125]

D *Health Information Security Regulations to Supplement the Privacy Act*

This paper recommends that the OAIC work with the Australian Attorney-General to develop health information security regulations pursuant to the *Privacy Act*.[126] The *HIPAA* Security Rule is a useful starting point for developing such regulations. The US and Australia have different regulatory approaches to privacy; however, US-style health information security regulations would be consistent with Australia's privacy scheme.

1 *Contrasting Regulatory Approaches*

Australia has adopted a comprehensive principle-based approach to privacy regulations. The *Privacy Act* contains high-level principles of general application to the private and public sectors.[127] Principle-based regulations set out substantive objectives or outcomes. Principle-based regulations are lauded for their simplicity and flexibility; however, such simplicity means that such regulations are often vague and non-specific.[128] Conversely, the US has adopted a sectoral approach to privacy by enacting federal laws specific to certain industries and practices, such as the *HIPAA* for the healthcare industry and the *Gramm-Leach-Bliley Act*[129] for the financial

[123] Monash University (n 2) 1. As discussed above, encryption is not technically mandatory under the *HIPAA* Security Rule.
[124] Department of Home Affairs (n 1) 41.
[125] See CSIRO and AustCyber, *Cyber Security: A Roadmap to enable growth opportunities for Australia* (CSIRO, 2018) 36-38.
[126] *Privacy Act 1988* (Cth) s 100.
[127] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, 30 May 2008), 950.
[128] Julia Black, 'Forms and Paradoxes of Principles Based Regulation' (LSE Law, Society and Economy Working Paper Series WPS 13/2008, London School of Economics and Political Science, 23 September 2008) 15–16.
[129] Also known as the *Financial Services Modernization Act of 1999.*

sector. This has resulted in a patchwork of US laws and regulations that are often prescriptive.[130] Prescriptive regulations focus on process as opposed to outcome. Prescriptive regulations are favoured for their detail and precision, but are faulted for their complexity, potential for inconsistency, tendency to contain loopholes and inflexibility.[131] The *HIPAA* Privacy Rule and Breach Notification Rule are prime examples of prescriptive regulations. As these rules are specifically tailored for the healthcare industry, they contain detailed and explicit requirements that can be complex and inconsistent. The *HIPAA* Security Rule is different from the other *HIPAA* rules, as HHS intentionally made the rule less prescriptive and more flexible because of the evolving nature of cyber technologies and threats.[132]

Under the Security Rule, each *HIPAA* entity has the flexibility to choose the method by which it complies with the applicable security standard. This flexibility accommodates technological advances and allows each *HIPAA* entity to implement safeguards in a manner appropriate to its circumstances.[133] Of course, this flexibility has also been criticised. Wafa opines that the Security Rule should contain more granular security standards to ensure PHI is adequately protected.[134] For example, Wafa contends that the rule should require a specific type of encryption. Similarly, Hoffman and Podgurski argue that the Security Rule is too vague, and that this vagueness will allow covered entities without security expertise to implement insufficient safeguards.[135] The criticisms may have some merit; however, HHS and the OCR have actively published guidance and newsletters with detailed information regarding compliance with the Security Rule.[136] Arguably, US regulators have struck a reasonable balance between flexible regulation, specific guidance and active enforcement that has helped foster a culture of security within the US healthcare industry.

---

[130] Department of Commerce Internet Policy Taskforce, *Commercial Data Privacy and Innovation in the Internet Economy* (16 December 2010) 58-60 <https://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework>.

[131] Oliver Krackhardt, 'New Rules for Corporate Governance in the United States and Germany—A Model for New Zealand' (2005) 36 *Victoria University of Wellington Law Review* 319, 330–31; Black (n 128) 16.

[132] 68 Fed Reg 8334, 8336-8338 (20 February 2003).

[133] Ibid.

[134] Tim Wafa, 'How the Lack of Prescriptive Technical Granularity in *HIPAA* Has Compromised Patient Privacy' (2010) 30(3) *North Illinois University Law Review* 531, 541–47.

[135] Sharona Hoffman and Andy Podgurski, 'In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information' (2007) 48(2) *Boston College Law Review* 331, 350-354, 370–82.

[136] US Department of Health and Human Services, *Security Rule Guidance Material* (Web Page) <https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>; US Department of Health & Human Services, *Cyber Security Guidance Material* (Web Page) <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html>.

2 *Hybrid Regulatory Approach*

The OAIC should seek to foster a culture of health information security by adopting a balanced approach as US regulators did with the Security Rule. However, it is challenging to achieve this balance relying on APP 11 and high-level guidance alone, as there must be close engagement between the regulator and regulated if principle-based regulations are to be effective. As Black explains, a regulator must convey and elucidate required outcomes and goals and implement a predictable enforcement regime to ensure compliance with principle-based regulations.[137] The OAIC has provided some guidance regarding compliance with APP 11; however, this guidance does not provide detailed and specific security outcomes that must be implemented to comply with APP 11.[138] Consequently, it is difficult for the OAIC to identify non-compliance and take appropriate action.[139] Detailed health information security regulations could help address this issue by conveying required security outcomes to healthcare organisations and providing the OAIC with specific standards for enforcement.

According to Black, a tiered approach provides the most effective means of regulation. When principle-based regulations are underpinned by detailed rules, a regulator can find the right balance between clarity and flexibility, simplicity and specificity.[140] The Australian Law Reform Commission ('ALRC') endorsed this type of hybrid approach for Australia's privacy regime. In 2008, the ALRC envisaged a regime comprising three tiers: the *Privacy Act*; the supplementary rules (as necessary); and guidance materials. The ALRC acknowledged that certain sectors, such as the health sector, may need supplementary rules. In such circumstances, it would be appropriate for the *Privacy Act* to be supplemented by more detailed rules.[141] Thus, health information security regulation is consistent with the hybrid approach envisaged by the ALRC and necessary to ensure the effective regulation of the health sector.

A hybrid approach to privacy is starting to develop in Australia under the Consumer Data Right ('CDR').[142] Presently, the CDR applies only to the banking sector, which must handle CDR data in accordance with the CDR's 'privacy safeguards' (based on the APPs of the *Privacy Act*).[143] The CDR privacy principles are supplemented by rules, including specific requirements for the security of CDR data.[144] These security requirements are extensive and require a formal

[137] Black (n 128) 4.
[138] See Siganto (n 20) 174–76.
[139] Ibid 114.
[140] Black (n 128) 7, 16.
[141] Australian Law Reform Commission (n 127) 240–43.
[142] *Treasury Laws Amendment (Consumer Data Right) Bill 2019* (Cth).
[143] *Competition and Consumer Act 2010* (Cth) ss 56EA, 56ED–56EP.
[144] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) sch 2.

information security governance framework and associated policies and procedures. The rules also require a formal information security controls assessment program and procedures and practices to detect and manage information security incidents. Additionally, certain information security controls must be implemented and a formal security training and awareness program adopted.[145] Similar security regulations should be developed by the health sector to ensure its unique security issues are addressed.

Regulators may feel trepidatious about introducing separate security regulations for the health sector given that past attempts for a distinct healthcare privacy regime have been controversial.[146] However, this paper does not propose that a separate privacy regime be introduced for the health sector; rather, it recommends that detailed health information security regulations be introduced that expound on the concise security principles contained in APP 11 of the *Privacy Act*. Australian health information security regulations would provide healthcare organisations with more direction and specificity for the purposes of safeguarding health information in accordance with the security principles under APP 11. This should minimise the number of healthcare breaches.

The *HIPAA* Security Rule provides a solid basis for developing Australian health information security regulations because it is tailored for the healthcare industry and has inbuilt flexibility. Like the Security Rule, Australian health information security regulations could provide healthcare organisations with flexible means of complying with security requirements. Carefully crafted Australian health information security regulations would augment APP 11 by accounting for the unique characteristics of the Australian healthcare industry and setting clear security standards for healthcare organisations to meet their obligations under APP 11. The regulations could accommodate changes in technology and each organisation's unique circumstances. The regulations could also enumerate contractual security requirements for third-party providers who handle health information. The regulations' effectiveness could be bolstered by supplementary guidance from the OAIC, compliance audits, fines, and corrective action for non-compliance. In providing guidance in support of the regulations, the OAIC could create a crosswalk to link the regulations' security requirements with the NESAF or other security frameworks as it deems appropriate.

[145] Ibid sch 2 rr 1.3–1.7, 2.2.
[146] Australian Law Reform Commission (n 128) 2030–38.

The inclusion of state and territory healthcare providers within the purview of Australian health information security regulations would further assist in bolstering health information security in Australia; however, any further discussion of this issue falls beyond the scope of this paper.

E *Modifications to the NDB Scheme Could Bolster the Enforcement of Health Information Security Regulations*

The Morrison Government's pending amendments to strengthen the enforcement of the NDB scheme could help mitigate privacy breaches. Going forward, it may be useful to adapt the NDB scheme to capture all incidents that compromise health information, regardless of serious harm. There is some concern that a lower notification threshold may cause notification fatigue. However, the harm standard creates opportunities for organisations represented by shrewd counsel to analyse their way out of reporting breaches that actually compromise the security and privacy of individuals' health information. Removing the harm standard under the *HIPAA* Breach Notification Rule generally made *HIPAA* entities feel more accountable, which contributed to greater *HIPAA* compliance.[147] It would also better enable the OAIC to identify any breaches resulting from failures to comply with health information security regulations.

The OAIC might also consider introducing specific deadlines that set clear due dates by which breach notifications must be issued. Additionally, if the OAIC lists breaches on its website (as the OCR does via the *HIPAA* 'wall of shame'), this might create a strong reputational incentive for organisations to mitigate breaches. However, making changes to the NDB scheme will not, in and of itself, prevent or mitigate healthcare breaches without associated health information security regulations.[148] Increased security measures may also improve breach detection.[149]

VI CONCLUSION

Health information is increasingly at risk of cyber-attacks; thus, the importance of robust information security measures cannot be over emphasised. Compared to the US, Australia has a relatively high occurrence of healthcare data breaches. This is because the US healthcare

[147] Butler (n 81).
[148] Smyth (n 66).
[149] HIPAA Journal, 'Healthcare Cybersecurity' *Healthcare Data Breach Statistics* (Web Page) <https://www.hipaajournal.com/healthcare-data-breach-statistics/>.

industry has a culture of information security that is underpinned by stringent enforcement of the *HIPAA* Security Rule, especially where non-compliance results in a breach. Conversely, Australian healthcare organisations only have general security guidelines to follow and less stringent breach notification rules, which has led to less emphasis being placed on information security measures and training.

The Australian government's focus on the enforcement of the *Privacy Act* and the 2020 Cyber Security Strategy may act as a catalyst for the introduction of health information security regulations. This paper opines that thoughtfully crafted Australian health information security regulations are necessary to inform healthcare organisations' compliance with APP 11. These regulations would support and operate in harmony with the *Privacy Act*. Such an approach would help to foster a culture of security within the Australian health sector, thereby reducing the number of healthcare data breaches.

Like the *HIPAA* Security Rule, the proposed health information security regulations should be both comprehensive and flexible. The Security Rule provides a strong foundation for developing Australian health information security regulations because it has contributed to more robust information security within the US healthcare industry. This may be why Australian regulators and industry professionals already reference the Security Rule and associated US standards. Additionally, removing the NDB scheme's harm threshold would better enable the OAIC to identify healthcare breaches resulting from inadequate security measures and take appropriate enforcement action.

ACKNOWLEDGEMENTS

I would like to offer special thanks to Associate Professor Mark Burdon, Faculty of Law at Queensland University of Technology and lawyer and researcher Bianca R Phillips for their guidance.

September 2020