THE AGE OF CONSENT:
DIGITAL PHOTOGRAPHY AND PRIVACY
IN GENERAL HEALTHCARE PRACTICE

SCARLETTE DE LAVAINNE

This thesis is presented for the Honours degree of Bachelor of Laws at
Murdoch University, (WA) Australia
I hereby declare it is my own account of my research

19,356 words
(Excluding title pages, table of contents, footnotes, appendices and bibliography)

2016
My sincerest thanks and gratitude to my supervisors, Dr Jo Goodie and Dr Chris Dent for their guidance and support.

My gratitude to Dr Simon Kessell for offering insights into medical practice.
ABSTRACT

Digital photography can be invaluable in visually oriented medical practice. Providing a visual record, digital photographs aid diagnosis, monitor change and quantify response to therapy. Incorporating digital photography into general practice is growing easier. Widespread ownership of smartphones with inbuilt cameras has stimulated this practice. Smartphone cameras are simple and familiar to use, capture high resolution images that enhance the medical record, expedite advice and, ultimately, can improve patient care.

The development and use of the smartphone is part of a broad wave of accelerated technological change. That change, the information revolution of the last 30 years, has enabled the collection and dissemination of that information on a scale previously unimaginable. It has also changed how Australians treat personal privacy. Personal information can be instantaneously shared, with or without consent, with friends and strangers. Expectations of privacy in younger generations may have dropped, but for many Australians, protection of privacy has become more urgent.

In response, Australia has tried to unify its legal and regulatory approaches to privacy protection through recent amendments to the Privacy Act 1988 (Cth). The Australian Privacy Principles were introduced to clarify and govern how personal information, such as healthcare information, can be collected, used and disclosed. The central role of the doctor in the collection and use of healthcare information required specific guidance for the profession. This was achieved through the professional Code of Conduct regulated by the Australian Medical Board.

Despite these legislative and regulatory changes there appears to be a divergence between practitioners’ conduct and their legal and professional obligations when using clinical photography in their healthcare practice. Are doctors aware of the requirements of consent, use and disclosure, and storage security, as they apply to clinical photography? The relevant literature suggested they are not. To explore how technology has impacted privacy this paper examines how the Privacy Act...
1988 (Cth) affects digital photography used in the clinical management of skin conditions. The paper will describe how well-delineated boundaries of clinical information sharing are blurred in practice, if not in law. It seeks to address the reasons for the apparent knowledge deficit of privacy obligations amongst practitioners.

Doctors looking to understand their privacy obligations will find it difficult; inconsistencies between laws and regulations making the regime challenging to traverse. This paper proposes possible solutions to raising awareness, promoting safer practices and can help mitigate privacy risks. Compliant use of digital photography is a value clinical tool which can facilitate patient care, while not endangering patient privacy.
# TABLE OF CONTENTS

## I INTRODUCTION ................................................................. 1  
   A Overview of this Thesis Paper ........................................ 1  
   B Outline of this Thesis Paper .......................................... 6  

## II PRIVACY, CONFIDENTIALITY AND CONSENT ...................... 8  
   A The Importance of Privacy, Confidentiality and Consent .......... 9  

## III PRIVACY PROBLEMS WITH DIGITAL PHOTOGRAPHY IN HEALTHCARE ................................................................. 15  
   A Digital Photography, Electronic Medical Records and the Law .... 15  
   B Issues of Consent and Record Keeping .............................. 19  
   C The Issue of Identifiability ........................................... 24  
   D Portable Devices and Clinical Photography ........................ 27  
   E Security Issues of Digital Clinical Photography ................... 29  
   F Loss of Control – ‘Information Drift’ ................................ 33  
   G The Effects of Social Media on Attitudes Towards Privacy ...... 34  

## IV REGULATORY BODIES AND CODES OF CONDUCT .................. 37  
   A The Introduction of the Modern Professional Code ............... 37  
   B The Role of Professional Codes in Healthcare Regulation ....... 38  
   C Confidentiality and Professional Codes ............................. 40  
   D The Australian Health Practitioner Regulation Agency (AHPRA) ... 42  
   E The Medical Board of Australia (MBA) ............................ 43  
   F The Royal Australian College of General Practitioners (RACGP) .... 44  
      1 An Overview of the RACGP .......................................... 44  
      2 RACGP ‘Standards for General Practice’ ........................... 45  
      3 RACGP Guidelines – What is Missing? ............................ 46  
   G The Australian Medical Association (AMA) ....................... 47  

## V FEDERAL PRIVACY LEGISLATION ......................................... 50  
   A Background of the Privacy Act 1988 (Cth) ......................... 51  
   B The Australian Law Reform Commission: Report 108 .............. 52  
   C The Privacy Amendment (Enhancing Privacy Protection) Act 2012 .... 53  
      1 Australian Privacy Principles (APPs) ............................ 56
VI CONCLUSION .................................................................................................................. 72
A The Problem Re-visited .......................................................................................... 72
B Increased Education - A Proactive Approach ...................................................... 72
C Indoctrination of Hospital-based Junior Doctors .............................................. 74
D Continuing Professional Development Training ............................................. 75
E Final Comments ........................................................................................................ 76

VII ANNEXURES .............................................................................................................. 79
Annexure A ..................................................................................................................... 79
Annexure B ..................................................................................................................... 80

VIII GLOSSARY OF TERMS .......................................................................................... 81

IX ACRONYMS .................................................................................................................. 85

X BIBLIOGRAPHY ........................................................................................................... 87
A Articles/Books/Reports ......................................................................................... 87
B Cases ............................................................................................................................. 94
C Legislation ................................................................................................................... 95
D Treaties ........................................................................................................................ 97
E Other ............................................................................................................................ 97
I INTRODUCTION

A Overview of this Thesis Paper

Since the original enactment of the Privacy Act 1988 (Cth) (the ‘Privacy Act’), Australia has participated in the global information and technology revolution. The speed and extent of this advancement has had its costs. The behaviours associated with technology adoption, the manner in which technological tools have been used over the last 30 years has often eroded personal privacy. The customs and assumptions that give cohesion to the community, the mores, have changed. In response, the Privacy Act was substantially reformed in 2014 and the Australian Privacy Principles (‘APPs’) were introduced. The APPs govern how personal information can be collected, used and disclosed.

Using the framework of the Privacy Act, this paper will examine how the adoption of technology in healthcare has brought specialist capabilities to general practice but threatened well-established professional privacy standards. By focusing on a microcosm of contemporary healthcare practice, the use of digital photography in the management of skin conditions, the case will be argued that a dichotomy exists between doctors’ conduct and their legal and professional obligations. Are doctors unaware or simply indifferent to the potential consequences to their actions? This paper will seek to answer this central question.

Core issues of privacy and confidentiality, consent, documentation, use and disclosure, de-identification and portability and storage security will be examined in this paper. It will also suggest that safer practices, improved awareness, and heightened concern of doctors can help mitigate the associated risks and promote compliance with regulatory requirements.

There appears to be a growing trend amongst medical practitioners to use digital photography in their healthcare practice.¹ Photography records description far more accurately than text. Comparisons of current and past images reveal visual changes

more dependably than memory or descriptive text.\(^2\) Radiologists, for example, use past images rather than rely on text reports to recognise change. General practitioners (‘GPs’) can enlist specialists in diagnostic dilemmas by sending photographs to dermatologists, plastic surgeons or pathologists who may give guidance, reducing the delay between correct diagnosis and treatment.\(^3\)

The relevant literature suggests, however, doctors’ use of clinical photography has outstripped their awareness or concern about privacy requirements. Hospital doctors who would not perform a procedure on a patient without disclosing risks and obtaining written consent often do not consider either disclosure or express consent necessary when clinical photographs are taken on their smartphone. Even when consent is obtained documentation appears to be lax and therefore unreliable.\(^4\) The same practice is likely true of GPs who work in a more relaxed and reassuringly familiar environment without benefit of a hospital’s legal and IT infrastructure, nor its budget for regulatory compliance. Whether through ignorance or complacency, patients’ privacy is at risk. Are medical practitioners aware of the many legal issues that arise when they incorporate digital photography into their healthcare practice?\(^5\) The relevant literature suggests that they are not.\(^6\)

Unlike film, digital photographs can be instantaneously and widely disseminated\(^7\) through wireless or internet-based transmission.\(^8\) Previously single function devices, camera, smartphone, computer, fax, have merged into devices which do and are connected to all. Social media accelerated device sharing between the personal and


\(^5\) Burns and Belton, above n 1, 265.


\(^8\) Stevenson, Finnane and Soyer, above n 4, 198.
The boundary between professional and personal network use is fluid. What can be done to protect personal privacy in this technologically dependent climate?

The specific focus of the paper on digital clinical photography is a consideration of the interaction between social habits and technological integration. This is most evident in the prolific and indiscriminate use not only of social media but also of email, texting and chatting applications, all of which are capable of instantaneous image distribution. This interaction in turn informs the discussion on current attitudes towards the safety and privacy of digital information. The paper will describe how well-delineated boundaries of clinical information sharing are blurred in practice, if not in law. It will be argued that practitioner awareness of, and concern about, legal privacy obligations must be raised if the risk of privacy breaches is to be reduced, consistent with the goals of the Privacy Act.

Digital photography can be invaluable in visually oriented specialties, such as dermatology, cosmetic surgery, burns and wound care. Providing a visual record, digital photographs aid diagnosis, monitor change and quantify response to therapy. Skin rashes evolve in nature and distribution; moles may exhibit previously invisible malignant features, and the transformation of size, colour, symmetry and border shapes can be precisely documented. The photographic record provides visual confirmation of the correct surgical site. Before-and-after pictures can reassure patients who have undergone cosmetic surgery and circumvent dissatisfaction and legal conflict.

Incorporating digital photography into general practice is growing easier. Widespread ownership of smartphones with inbuilt cameras has stimulated the use of

---

9 National Nurse, HIPAA – The Health Insurance Portability and Accountability Act: What RNs Need to Know About Privacy Rules and Protected Electronic Health Information <http://nurses.3cdn.net/9480c5f552f052a8e5_vsm6bp9vu.pdf>.
10 Graham Scott, ‘Social Media is Blurring Professional Boundaries’ 2013 27(52) Nursing Standard 1,1; Sánchez Abril, Levin and Del Riego, above n 7, 64.
11 Burns and Belton, above n 1, 265; Matthew Lenardis, Robert Solomon and Fok-Han Leung, ‘Store and Forward Teledermatology: A Case Study’ (2014) 7 BioMed Central Research Notes 588, 588.
13 Van der Rijt and Hoffman, above n 6, 211.
14 Ibid.
15 Scheinfeld et al, above n 1, 822.
digital photography by medical practitioners. Directly or with adapters, smart phone cameras can capture images, which can be uploaded into patient records or emailed to an authority for advice. The simplicity and familiarity of the process facilitates the addition of clinical pictures.

Medical practitioners are legally required to maintain patient privacy and confidentiality. Identifiable clinical photographs form part of a patient’s medical record and therefore, attract the same protection as a written record. Collection, use and disclosure require patient consent. The obligation exists in the APPs and the Medical Board of Australia’s mandatory Code of Conduct (the ‘Code’). Consent ensures that the patient maintains control over how the information can be used: it is a controlling condition. It is inextricably linked to privacy and confidentiality, and essential to the doctor-patient relationship. All protections, legal and regulatory, apply equally to personal information, including identifiable clinical photographs.

Clinical photography is a deceptively harmless practice that raises many privacy concerns. Inadequate security precautions put patients’ sensitive information at risk, when retained on the camera device, transferred to a computer, sent via the internet, or stored by an ‘cloud’ provider. This can be especially troubling when the online cloud provider may be foreign or their storage facilities physically located offshore, where Australia privacy standards do not apply.

17 For example, the ‘Mole Scope’ iPhone adapter $99 USD; MoleScope, Products <https://molescope.com/product/>.
18 Stevenson, Finnane and Soyer, above n 4, 198.
20 This paper uses the terms ‘medical practitioner’, ‘practitioner’ and ‘doctor’ interchangeably.
22 Ibid s 6FA(b) defines ‘health information’ as ‘other personal information collected to provide, or in providing, a health service’; Mahar et al, above n 17, 48; Kirk et al, ‘The Role of Smartphones in the Recording and Dissemination of Medical Images’ 2014 3(2) Journal of Mobile Technology in Medicine 40, 41; Catherine Hood, Tony Hope and Phillip Dove, ‘Videos, Photographs and Patient Consent’ 1998 316 British Medical Journal 1009, 1009.
23 Ibid.
24 Privacy Act 1988 (Cth) sch 1 pt 3 cl 6.
25 Ibid.
27 Above n 23.
28 Nielson, West and Shimizu, above n 20, 1-2.
Using a personal device to take clinical photographs increases the likelihood of breach. Smartphones are often set to backup or synchronise data with other devices or personal cloud storage, leading to transfer of clinical images beyond a medical practice’s protection.\textsuperscript{29} If the backup or synchronisation account is shared with a family member, a privacy breach is almost inescapable. Importing personal devices into clinical settings can significantly amplify the risk of breach.

Medical practitioners are, generally, cognisant of their legal and professional obligations concerning patient privacy.\textsuperscript{30} Most modern English versions of the Hippocratic Oath, voluntarily taken by medical graduates, include the sentiment that the new doctor ‘will respect the privacy … of patients’.\textsuperscript{31} The legal obligations are clearly described in the Medical Board of Australia’s Code,\textsuperscript{32} yet are frequently disregarded.

The Australian Medical Association (‘AMA’) has issued a ‘Clinical Photography Guide’, which provides a straightforward explanation of how to manage clinical photography on mobile devices. It explains the core issues and alerts doctors to the risk of fines in addition to AHPRA\textsuperscript{33} sanctions. It is an excellent prescriptive guide. It is also not widely circulated to GPs, few of whom know of its existence. The necessity for this guide highlights the difficulty for those GPs who want to understand their privacy obligations. These requirements are spread across a disparate body of commonwealth and state laws and regulations, including professional codes of conduct and guidelines. They are not conveniently located in one act. Some of these impose contradictory obligations on the medical profession. One goal of this paper is to clarify and reconcile these obligations by providing a comprehensive overview of the regulations and describe a practical course for doctors who want to meet their privacy obligations while incorporating clinical photographs into their professional practice.

\textsuperscript{29} Ibid 2.
\textsuperscript{30} This awareness stems from the modern day version of the Hippocratic oath, versions of which have been adopted in medical codes of conduct; Ruth Purtilo, Ethical Dimensions in the Health Professions (Elsevier Saunders, 4th ed, 2005) 172; Sonia Allan and Meredith Blake, The Patient and the Practitioner: Health Law and Ethics in Australia (LexisNexis Butterworths Australia, 2014) 298.
\textsuperscript{33} Australian Health Practitioner Regulation Agency (AHPRA).
What role does the Office of Australian Information Commission (‘OAIC’) have in improving the situation? Should the Privacy Commissioner take a harsher approach by increasingly seeking civil penalty orders for proven breaches? Would this increase awareness of privacy obligations and security practices? Or would it effectively proscribe the practice of clinical photography denying patients and doctors the benefits of a valuable diagnostic and management tool? There are insufficient determinations by the Privacy Commissioner to examine the issue adequately.  

These issues are not unique to Australia; similar legislative changes have been enacted overseas, the most comprehensive and forceful is seen in the United States (‘US’). Historically, it is not uncommon for healthcare practices and regulations to develop in Australia only after they have appeared in some form in the US. Presently, no Australian case law exists. If the proposed mandatory data breach notification bill is enacted, however, Australia is likely to follow the US, where compulsory notification of privacy breaches involving health information has led to an upsurge of privacy-related litigation, settlements and regulatory fines. The current Australian civil penalty for serious breach of privacy can be up to $1.8 million.

Why then, do medical practitioners not appear to apply the same standards of privacy and confidentiality to digital photographic information as they give to physical data? To answer this question, it is necessary to understand the problem.

B Outline of this Thesis Paper

Chapter II examines the roles of privacy, confidentiality and consent within healthcare. Chapter III reviews the challenges of digital photography in clinical practice. It reveals that core principles of patient confidentiality and consent may be

---


35 The Health Insurance Portability and Accountability Act of 1996 (‘HIPAA’), Privacy, Security, Enforcement and Breach Notification Rules, in accordance with the Health Information Technology for Economic and Clinical Health Act of 2009 (‘HITECH’) govern how ‘personal health information’ (‘PHI’) is handled.

36 For example, the US Privacy Act of 1974 was enacted 14 years ahead of the Australian equivalent Privacy Act 1988 (Cth).

overlooked and privacy disregarded. This leads to an analysis of scenarios that magnify the security risks created when safe management of clinical photographs is compromised.

Chapter IV deconstructs the relevant regulatory system by exploring each body’s powers, limitations and level of influence over practitioners. Chapter V is a close analysis of the Privacy Act, especially the 2014 amendments introduced following the recommendations of the Australian Law Reform Commission (‘ALRC’). These amendments were developed to deal with the evolution of online behaviours and technological capabilities so disruptive to previous social norms that individual privacy can be so easily put at risk.

Chapter VI concludes by identifying the key factors that oppose complete protection of patient privacy. It admits the adequacy of the law and emphasises the difficulties in changing the practices and habits of doctors who use digital photography. Recommendations are made for how professional practices, assumptions and attitudes might be transformed to ensure patient privacy as required by law.
II PRIVACY, CONFIDENTIALITY AND CONSENT

Privacy and confidentiality are separate concepts, though there is considerable overlap and the terms are often mistakenly used synonymously. Privacy refers to an individual’s right to control of his or her own personal information. Based on a respect for individual autonomy, privacy reflects the ability to determine who gets to know what about oneself; for example a person may wish to shield certain information from public view. Confidentiality, on the other hand, acts as a conditional agreement by which one party consents to pass information on to a second party on the mutual understanding that neither the information, nor the source of the information, will be disclosed or divulged to a third party without the consent of the originating source. The agreement may be explicit, as in a verbal or written promise or contract, or implicit, due to the nature of the relationship between the source and receiving parties. Privacy arises from, and is determined directly by, an individual, whereas confidentiality can only exist within the context of a particular relationship. Confidentiality is the obligation of the receiver, to the giver of the information.

The relationship between a doctor and a patient, has been recognised historically, ethically, and statutorily as creating the obligation of confidentiality from the doctor to the patient. However, if a doctor breaches patient confidentiality by failing to obtain the patient’s consent before disclosing personal information, that practitioner also invades the patient’s privacy.

As will be discussed, the doctor has a legal duty of care not only to avoid active disclosure of information received in confidence, but also to ensure that this information is secure from inadvertent disclosure, unauthorised access or theft. The

38 Ian Kerridge, Michael Lowe and John McPhee, Ethics and Law for the Health Professions (The Federation Press, 2nd ed, 2005) 244.
40 Attorney General v Guardian Newspapers Ltd (No. 2) [1988] 3 All ER 545, 27 (Lord Goff); Kerridge, Lowe and McPhee, above n 38, 237.
41 Purtilo, above n 30, 175; Dhai Amaboo and Jason Payne-James, ‘Problems of Capacity, Consent and Confidentiality’ 2013 27 Best Practice & Research Clinical Obstetrics and Gynaecology 59, 67.
42 Berle, above n 42, 107.
43 Medical Board of Australia, above n 26.
requirement to maintain ‘accurate, up-to-date…records’ creates an increasingly complex technological obligation; from filing cabinets, padlocks and locked doors to computer systems, networks and data storage with passwords, access restrictions, and encrypted data transmissions. The greater simplicity of using more sophisticated resources, such as electronic reports or digital images, can beguile the practitioner into complacency, non-compliance and breach.

A The Importance of Privacy, Confidentiality and Consent

To provide complete and honest information a patient must feel that his or her person and personal information can be safely entrusted to the medical practitioner. Private information may be intimate or embarrassing yet essential to receiving appropriate care. The patient’s decision to reveal this information relies upon his or her freely given consent. The a priori need for this consent arises from the ‘respect for patient autonomy… a fundamental principle in contemporary bioethics’. Beauchamp and Childress, pioneers of biomedical ethics, define autonomy as ‘self-rule that is free from both controlling influence by others and from certain limitations, such as inadequate understanding, that prevent meaningful choice’. The patient retains the right to autonomy over his or her own body; to act contrary to a patient’s wishes may cause the patient harm. The medical practitioner remains dependent upon the patient’s continuous grant of consent and is obligated to safeguard from disclosure anything the patient has revealed. This grant of consent

44 Ibid.
46 Kerridge, Lowe and McPhee, above n 38, 219.
50 Berle, above n 47, 43; Berle, above n 47, 90.
51 For the ‘Duty of Confidentiality’ see Coco v AN Clark (Engineers) Ltd [1969] RPC 41 [47]; see also Richards v Kadian [2008] NSWCA 328 as cited by Kerridge, Lowe and McPhee, above n 38, 236-8.
is made by the patient, in exchange for the practitioner’s obligation of confidentiality.

The reliance of the patient-practitioner relationship upon a foundation of confidentiality, was recognised over 25 centuries ago. In the first records of the ‘Hippocratic Oath’ physicians vow:

‘And whatsoever I shall see or hear in my course of my profession, as well as outside my profession … if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets.’

_Private_ information that is communicated by the patient to the medical practitioner is protected by _confidentiality_. Private information about patients may be ‘appropriately’ shared ‘for their healthcare’ though only if done in a manner ‘consistent with privacy laws and professional guidelines’. The treating practitioner still needs to exercise discretion, disclosing only relevant information to other medical practitioners who may assist in the patient’s care. The obligation of confidentiality and most of the Australian Privacy Principles (‘APPs’), established by the _Privacy Act 1988_ (Cth) (‘Privacy Act’), will then attach to the disclosed information, continuing to provide protection. This principle of ‘secondary’ disclosure is recognised in APP 6. If ‘the individual would reasonably expect’ that disclosure supports the ‘primary purpose’ of improving the patient’s health, the information may be disclosed. This goal is explicitly defined within the context of providing a ‘health service’ which is intended to ‘assess, maintain or improve the individual’s health’ or diagnose’ or ‘treat’ an ‘illness, disability or injury’.

In circumstances where several people are involved in the provision of health services it is not possible, nor reasonable for the primary practitioner to seek consent for each disclosure. APP 6, dealing with use and disclosure allows for such instances,

---

52 Purtilo, above n 30, 172; Allan and Blake, above n 30, 298.
53 In this context the term ‘physician’ differs from the contemporary medical definition used in Australia. Use of the term physician is intended to have the same definition as ‘medical practitioner’.
54 Purtilo, above n 30, 172.
56 Medical Board of Australia, above n 26.
57 _Privacy Act 1988_ (Cth) sch 1 pt 2 sub–cl 4.4.
58 Ibid sch 1 pt 3 sub–cl 6.2(a).
59 Ibid s 6FB ‘Meaning of health service’.
specifying a practitioner is only authorised to use or disclose the information (e.g. clinical photographs) for a purpose directly related to the primary purpose the information was collected for. The majority of patients appreciate the need to balance these tensions, accepting this type of disclosure appropriate in the context of clinical photographs. Where a practitioner wishes to disclose confidential information outside of these boundaries, they must seek the patient’s valid consent.

In order for consent to be valid, all material information must be disclosed to the patient and he or she must have the legal capacity to understand what is being consented to, including the benefits, risks, likely outcome, and in some cases, possible alternatives. Clinical photographs pose different risks to that associated with medical treatment, such as breach of privacy through unauthorised access, use or disclosure, nevertheless the patient should be given adequate information to make an informed decision. Additionally, the consent must be specific, that it, consent must be given to a specific act or treatment and cannot be a ‘blanket’ agreement, and it must be granted freely and without coercion. It is highly recommended that practitioners, who obtain patient consent to use and disclose clinical photographs for educational or publishing purposes, ensure consent is in written form. Although patients may withdraw consent at any time, it is essential the patient understands that once images have entered the public domain the images are likely irretrievable.

---

60 Ibid sch 1 pt 3 cl 6.
63 Legal capacity is not ‘static’ and must be assessed in the relevant context. Capacity is presumed unless it is proved otherwise; Ben White, Fiona McDonald and Lindy Willmott, Health Law in Australia (Thomson Reuters (Professional) Australia Limited, 2nd ed, 2014) 133; See, eg. Re C (Adult: Refusal of Medical Treatment) [1994] 1 WLR 290.
64 F v West Berkshire Health Authority [1989] 2 All ER 545.
65 Lakdawala, Fontanella and Grant-Kels, above n 2, 486.
66 Berle, above n 42, 107.
67 Murray v McMurphy [1949] 2 DLR 442.
68 Davis and Barking, Havering and Brentwood Health Authority (1993) 4 Med LR 85 as cited by Kerridge, Lowe and McPhee, above n 38, 284.
69 Re T (Adult: Refusal of Treatment) [1993] Fam 95.
Despite the importance consent plays in respecting patient autonomy and confidentiality, often insufficient attention is given to the process of obtaining patient consent. Clinical photography may leave an already vulnerable patient feeling objectified if their right to autonomy is disrespected. Still, it is not uncommon for practitioners to rely on implied consent for clinical photography. As implied consent is not defined, it may be open to interpretational discrepancies between patient and practitioner. A patient’s understanding of what he or she consented to may not align with the practitioner’s understanding. For example, as Royal London Hospital’s medical photographer, Ian Berle explains, some patients will expect that photographs taken be for documentation purposes only. As explained above, the Privacy Act allows the primary practitioner to use and disclose the patient’s photographs for a secondary purpose ‘directly related’ to the primary purpose provided this is what a patient would ‘reasonably expect’ (for example, to seek diagnostic assistance from a colleague). A patient may feel, however, that privacy has been breached, if the medical practitioner has dealt with the photographs in a way contrary to the patient’s expectations. While the practitioner’s actions may be within the bounds of the Privacy Act, consent which is both explicit and clearly defined is likely to prevent both misunderstanding and unintentional misuse.

The power structure of the doctor-patient relationship is widely acknowledged to be unequal. Patients render themselves vulnerable through their personal revelations of weakness and, often, fear. Reluctance to be so exposed is usually overcome because of trust in the practitioner’s beneficence, the expectation that the practitioner, unless provoked, acts primarily in the patient’s best interest. A

---

75 Lauren Kunde, Erin McMeniman and Malcolm Parker, ‘Clinical Photography in Dermatology: Ethical and Medico-legal Considerations in the Age of Digital and Smartphone Technology’ 2013 54 Australasian Journal of Dermatology 192, 194; Kornhaber, Betihavas and Berber, above n 6, 300; Scheinfeld and Rothstein, above n 73, 199.
76 Allan and Blake, above n 30, 65.
77 Berle, above n 47, 89.
78 Privacy Act 1988 (Cth) sch 1 pt 3 cl 6.
80 Lau, Schumacher and Irwin, above n 61, e508-10.
81 Medical Board of Australia, above n 26; A Better NHS, Medical Power (5 October 2012) <https://abetternhs.net/2012/10/05/medical-power/>.
vulnerable patient\textsuperscript{82} may accept personally unpalatable behaviour if refusal to comply is felt to be either impossible or counterproductive to receiving the best care,\textsuperscript{83} undermining genuine ‘voluntary’ consent. Presented by the doctor as a statement of intent or need, ‘I will’, ‘I should’, ‘Is it alright if I…’, implicitly relies on the imbalance in power. The patient’s quiescence, motivated by faith, trust and fear of uncertainty, may be seen, as Berle interprets it, as ‘passive coercion’.\textsuperscript{84} The medical practitioner has a duty, according to this argument, to allow the patient to make a self-determined decision: to recognise and maintain the patient’s autonomy.

Central to autonomy is respect for self-governance, rights to liberty and privacy and the freedom of independent choice.\textsuperscript{85} The right to retain control over private information requires confidentiality.\textsuperscript{86} Confidentiality, however, did not always respect patient autonomy. Physicians saw themselves, since at least the time of the creation of the Hippocratic Oath, as the best judge of the risk to the patient regarding disclosure of personal information, and who may be entrusted with its safe-keeping.\textsuperscript{87} Patients, themselves, were not necessarily included in the chain of communication if the physician felt that knowledge of their prognosis may worsen their condition or causes them needless suffering. Thus, relatives of terminally ill patients, after being informed, were asked to conceal the true nature of their disease.\textsuperscript{88} Until the latter part of the twentieth century, the chain of communication was usually paternalistic reinforcing societal conventions regarding women as lacking the capacity for self-determination.\textsuperscript{89} They simply did not have the emotional or moral courage, or the rational capacity to be told what was happening to them. It was not in their ‘best interest’.\textsuperscript{90} Thomas Percival, an English physician at the beginning of the 19\textsuperscript{th} century, has been recognised as drafting the first modern (medical) professional code of ethics.\textsuperscript{91} His code, which was later adapted and adopted by the American Medical Association, was not based on patient autonomy, however, but on the physician’s

\textsuperscript{82} Berle, above n 47, 43; Berle, above n 47, 90.
\textsuperscript{83} Burns and Belton, above n 1, 265; Berle, above n 47, 90.
\textsuperscript{84} Berle, above n 47, 90.
\textsuperscript{85} Amaboo and Payne-James, above n 41, 60.
\textsuperscript{86} Lockwood, above n 45, 107.
\textsuperscript{88} Ibid.
\textsuperscript{90} Lockwood, above n 45, 107.
\textsuperscript{91} Higgins, above n 87, 923.
‘honour’. 92 To some critics, his code would seem more protective of the physician’s honour and prerogative rather than those of the patient.93

Information ‘disclosure’ touches not only on confidentiality, the right to control who knows what about oneself, but also on one’s own ability to make informed decisions, to give ‘informed consent’. If you are not made aware of the risks, can you really understand to what you are consenting?

---

92 Higgins, above n 87, 923.
III PRIVACY PROBLEMS WITH DIGITAL PHOTOGRAPHY IN HEALTHCARE

A Digital Photography, Electronic Medical Records and the Law

The Australian healthcare sector, particularly medical practices, is becoming a target for cybercrime. Unlike financial account details, stolen health information cannot be replaced for uncompromised data. An estimated 7.5% of patients in the United States will fall victim to personal healthcare data theft within the next 5 years. One third of all data breaches reported in 2015 occurred in the health/medical sector. Mandatory reporting of breach incidents has led to more litigation suits and successively heavier regulatory fines.

Australian healthcare organisations’ vulnerability is no less concerning. The Australian Financial Review reported that neglectful or weak data security places these organisations ‘next in the firing line’. This has not gone unnoticed. Last year (2015), in Australia, the Security and Intelligence Joint Committee recommended compulsory reporting for all serious data breaches. The vast majority of Australian online participants support compulsory reporting when a data breach occurs. The ‘Privacy Amendment (Notification of Serious Data Breaches) Bill 2016 (Cth) is due before Parliament in the Spring 2016 sitting. If enacted, Australian healthcare providers may be confronted by litigation and regulatory fines for serious data breaches similar to that seen in the US. For a recent serious health information

---

96 Pillay, above n 95.
100 Centre for Internet Safety, University of Canberra, Privacy and the Internet: Australian Attitudes Towards Privacy in the Online Environment <http://www.canberra.edu.au/cis/storage/Australian%20Attitudes%20Towards%20Privacy%20Online.pdf>
101 Pillay, above n 95.
breach involving the Australian Red Cross Donor Bank, see the discussion in Chapter V.\textsuperscript{102}

Unlike the US and Canada,\textsuperscript{103} Australia does not recognise tortious invasion of privacy.\textsuperscript{104} Prior to the 2014 reform of the Privacy Act an aggrieved party had to seek recourse through breach of (implied) contract, the tort of negligence or equitable breach of confidence. Whether a cause of action was available depended on the circumstances of each case. The Privacy Act’s 2014 reform strengthened protection of individuals’ personal information.\textsuperscript{105} Several definitions in the Act have been updated: Clinical photographs, which form part of a patient’s medical record,\textsuperscript{106} are ‘health information’.\textsuperscript{107} Health information is now recognised as ‘sensitive information’ by the Federal public sector,\textsuperscript{108} affording it increased protection.\textsuperscript{109}

Stronger privacy protection laws allow fines of the breaching practitioner and employer up to $360,000 and $1.8 million respectively.\textsuperscript{110} Nevertheless, Australian doctors have not fully appreciated that clinical photography bears the full burden of privacy and confidentiality obligations.\textsuperscript{111} Junior doctors and trainees in hospitals frequently photograph patients when seeking diagnostic help from senior colleagues.\textsuperscript{112} Consent may be overlooked and hospital policies and guidelines ignored.\textsuperscript{113} Careless practices may cause significant harm to the patient through

\textsuperscript{102} See Ch 5, ‘Breach of the Privacy Act’ of this paper.
\textsuperscript{104} Victoria Park Racing and Recreation Grounds Company Limited v Taylor (1937) 58 CLR 479; John Fairfax Publications Pty Ltd v Hitchcock [2007] NSWCA 364 [123]; White, McDonald and Willmott, above n 63,129; although questionable, there have been two lower court cases that allowed recovery for breach of privacy; Grosse v Purvis [2003] QDC 151; Jane Doe v Australian Broadcasting Corporation [2007] VCC 281.
\textsuperscript{105} For example, more stringent limitations apply to how information can be collected, used and disclosed; Davis, above n 73, 117; see Privacy Act 1988 (Cth) sch 1 pt 2 cl 3, sch 1 pt 3, cl 6. Cross border disclosure and accountability also applies to disclosing entity; Privacy Act 1988 (Cth) sch 1 pt 3 cl 8.
\textsuperscript{106} Privacy Act 1988 (Cth) sch 1 pt 2 sub–cl 3.3, pt 3 sub–cl 6.1; Privacy Act 1988 (Cth) s 6 defines ‘record’ as a document, or electronic or other device. Medical records include ‘clinical notes, investigations, letters from other health providers, photographs and video footage’; MDA National, Medical Records <http://www.mdanational.com.au/~/media/Files/MDAN-Corp/Medico-Legal/Medical-Records.pdf?la=en>.
\textsuperscript{107} Privacy Act 1988 (Cth) s 6FA(b) defines ‘health information’ as ‘other personal information collected to provide, or in providing, a health service’.
\textsuperscript{108} Privacy Act 1988 (Cth) s 6 defines ‘sensitive information’ which includes ‘health information’; Australian Medical Association, above n 79.
\textsuperscript{109} Privacy Act 1988 (Cth) ss 6(1), sch 1 pt 2 sub-cls 3.3–3.4, sch 1 pt 2 sub-cl 6.2.
\textsuperscript{110} Privacy Act 1988 (Cth) ss 13G, 80W.
\textsuperscript{111} Kornhaber, Betihavas and Baber, above n 6, 301; Burns, above n 6, 14; Van der Rijt and Hoffman, above n 6, 212.
\textsuperscript{113} Kornhaber, Betihavas and Baber, above n 6, 301.
unauthorised use or disclosure of clinical photographs, which have the potential to embarrass or humiliate the patient. Despite these risks, clinical imagery can improve patient care.\textsuperscript{114}

Digital imaging can assist practitioners to identify the correct site location. Typically, when a patient questions the state of a lesion and the practitioner is unable to determine if it is benign or malignant, a biopsy is likely to be performed.\textsuperscript{115} Removing a small sample of the questionable tissue, it is sent for testing, where the pathology will reveal if it is necessary to excise the lesion.\textsuperscript{116} A shortage of qualified dermatologists have added to lengthy delays between biopsy and the dermatological surgery, leaving enough time for the small biopsy site to heal sufficiently, so that it cannot be easily located.\textsuperscript{117} The longer the delay between biopsy and full excision, the higher the chance of incorrect site identification,\textsuperscript{118} a frequent cause of medico-legal lawsuits.\textsuperscript{119} Erroneous site identification in one survey was a reported 14%.\textsuperscript{120} A dermatologic study investigated both patient and practitioner accuracy of locating the biopsy site. 16.6\% of patients and 5.9\% of physicians involved in the study identified the surgical site incorrectly.\textsuperscript{121}

Clinical photography, when used within the constraints of the law, offers a practical, effective solution to identify the correct site,\textsuperscript{122} protecting practitioners from lawsuits.\textsuperscript{123} Although de-identifying patients’ photographs is safer (for example by excluding anatomical landmarks, opting for macro shots, and excluding other important features from the frame) this may undermine the clinical utility of biopsy site photographs.\textsuperscript{124} Depending on the lesion’s placement, the photograph frame may

\textsuperscript{114} Stevenson, Finnane and Soyer, above n 4, 198.
\textsuperscript{116} Comfere et al, above n 115, 549.
\textsuperscript{118} McGinness and Goldstein, above n 117, 195.
\textsuperscript{120} Ibid 198.
\textsuperscript{121} McGinness and Goldstein, above n 117, 195.
\textsuperscript{122} Ke et al, above 119, 198; McGinness and Goldstein, above n 117, 194; Pharmacology and Therapeutics Panel Discussion, above n 115, 00:13:50.
\textsuperscript{123} McGinness and Goldstein, above n 117, 197.
\textsuperscript{124} Ibid 195.
require these anatomical landmarks (e.g. a patient’s facial features - lips, ears, nose and eyebrows) to provide reference points for future comparison.\(^\text{125}\)

Photography is not only used to photograph skin lesion, it has been found to be effective in ‘total body photography’, a method used to capture the body’s full form through a series of images.\(^\text{126}\) A physical skin examination of the entire body can be used to identify skin lesions that may present a risk of malignancy,\(^\text{127}\) and can be supplemented with photographic documentation to assists with ‘anatomically correct mapping’.\(^\text{128}\) The practice of ‘total body imaging’ is increasingly being used as it provides the practitioner with a ‘baseline’ comparison, allowing the discernment of slight changes, in patients who are predisposed to developing skin malignancies that may have otherwise gone unnoticed.\(^\text{129}\) Effective monitoring through photography can lead to early detection and treatment, however, total body imaging is recognised as a privacy threat due to the identifiability of patient photographs.\(^\text{130}\)

Sufficient privacy and security safeguards are absolutely essential given the sensitive nature of such images.

The prevalence of mobile phone ownership, which almost universally have inbuilt cameras,\(^\text{131}\) has simplified widespread use of digital photography within medicine.\(^\text{132}\) Almost 100% of medical practitioners surveyed in a recent study owned a mobile phone with an integrated camera, 89% of which had internet connectivity.\(^\text{133}\) A majority (65%) of respondents admitted taking clinical photographs with their phones. Consent was not obtained in 24% of those patients photographed. When consent was obtained, it was mostly verbal,\(^\text{134}\) and documentation was poor - only 23% recorded consent in the medical records.\(^\text{135}\) In another Australian study, all of the participating medical registrars used their phones to photograph patients.\(^\text{136}\)

---

\(^{125}\) Ibid; Pharmacology and Therapeutics Panel Discussion, above n 115, 00:15:51.

\(^{126}\) Scheinfeld and Rothstein, above n 73, 199.


\(^{129}\) Risser et al, above n 127, 429.

\(^{130}\) Lakdawala, Fontanella and Grant-Kels, above n 2, 487.

\(^{131}\) Van der Rijt and Hoffman, above n 6, 211.

\(^{132}\) Scheinfeld et al, above n 1, 822; Burns and Belton, above n 1, 265.

\(^{133}\) Kirk et al, above 23, 40-42.

\(^{134}\) Ibid 40-42; Privacy Act 1988 (Cth) sch 1 pt 2 sub–cl 3.3 outlines the ‘collection of sensitive information’

\(^{135}\) Ibid.

\(^{136}\) Kunde, McMeniman and Parker, above n 75, 193.
Smartphones enable doctors to ‘capture and transmit patient images’\(^{137}\) with a ‘high degree of autonomy’.\(^{138}\) Their use is simple, efficient and deceptively safe. The practice warrants examination. Is patient confidentiality and privacy jeopardised when an increasingly common behaviour is not accompanied by concomitant consent and security precautions? Do patients still have control over the use of their clinical images?

B Issues of Consent and Record Keeping

The doctrine of consent is well established and understood by healthcare providers.\(^{139}\) Based on the principle of patient autonomy, every patient has the ‘right of control and self-determination’ concerning his or her body.\(^{140}\) That right exists whether consent is used to perform a surgical procedure or take a personal photograph.\(^{141}\) Consent enables doctors to preserve patients’ privacy and confidentiality decisions.

The Privacy Act makes clear that medical practitioners who take ‘reasonably identifiable’\(^{142}\) patient photographs must first seek consent.\(^{143}\) The word ‘reasonable’ in the Privacy Act implies an objective standard,\(^{144}\) one that is well understood in most areas of law.\(^{145}\) That standard, when applied to identity, is not the subject of

---

\(^{137}\) Stevenson, Finnane and Soyer, above n 4, 198.


\(^{139}\) Schloendorf v Society of New York Hospital, 195 NE 92 (NY, 1914).

\(^{140}\) Secretary, Department of Health and Community Services (NT) v JWB (Marion’s case) (1992) 175 CLR 218 309-10 (McHugh J); Schloendorf v Society of New York Hospital, 195 NE 92 (NY, 1914); Hood, Hope and Dove, above n 23, 1009.


\(^{142}\) The Act does not define ‘reasonable identifiability’ and ‘reasonably identifiable’. The Explanatory Memorandum states the test is ‘to be based on factors which are relevant to the context and circumstances in which the information is collected and held’. It also encourages the OAIC to publish guidelines to assist entities in its application; Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 53.

\(^{143}\) Privacy Act 1988 (Cth) sch 1 pt 2 sub–cl 3.3 outlines the ‘collection of sensitive information’; Consent requirements are the same in the UK and the US; Hood, Hope and Dove, above n 23, 1009; Scheinfeld and Rothstein, above n 73, 200.

\(^{144}\) The Explanatory Memorandum reminds the reader that objectivity is to be determined in the light of the circumstances. For example, it states that the phrase ‘reasonable steps’ indicates that the circumstances and context must be considered. The memorandum also notes that objectivity is based on a ‘reasonable person’s perspective’, rather than the organisation concerned; Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 53, 54.

\(^{145}\) See, eg, ‘reasonable foreseeability’ as referred to in Wyong Shire Council v Shirt (1980) 146 CLR 40; also see ‘reasonable care’ as referred to in Donoghue v Stevenson [1932] AC 562 [580].
this thesis. It is worth mentioning, however, that in a world of big data analysis, fragments of information can be drawn together from disparate sources, such as social media, search words and phrases and email services that tailor advertising to email phrases or user relationships.\footnote{146} Like tiny pieces of a large jigsaw puzzle, an identifiable picture of an individual may be assembled.\footnote{147} What is not ‘reasonably identifiable’ today may become so in the future.\footnote{148} Will the courts’ understanding of ‘reasonableness’ change when it relates to ‘identifiable’?

The Privacy Act does not apply to de-identified information.\footnote{149} Consent for collection and use of information applies, under the Privacy Act, only for information that is ‘personal’; the individual from or about whom the information is collected must be ‘reasonably identifiable’.\footnote{150} Under the Privacy Act, ‘health information’ is information ‘collected to provide, or in providing, a ‘health service’\footnote{151} to an individual’ only if the information falls within the meaning of ‘personal information’.\footnote{152}

Use of a de-identified photograph originally taken during the provision of a health service would not, \emph{under the Privacy Act}, require patient consent. So what makes a photograph ‘de-identified’?

A photograph would be covered under the Privacy Act if it contained either \emph{recognisable content} or \emph{identifying metadata} (name, record number, date of birth), which allows the individual to be ‘reasonably identifiable.’ A photograph that has neither sufficiently recognisable content nor identifying metadata is ‘de-identified’

\begin{footnotesize}
\begin{enumerate}
\item[147] For example internet provider AOL released de-identified internet searches (which included searches for health related information) and a few days later the \textit{New York Times} published an article reporting that they had successfully re-identified customers based on the search data: Michael Barbaro and Tom Zellar, \textit{A Face is Exposed for AOL Searcher 4417749} (9 August 2006) New York Times <http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000&_r=0>.
\item[148] This was an issue raised in the ALRC report, concerning biometric ID, such as facial recognition; Australian Law Reform Commission, \textit{For Your Information: Australian Privacy Law and Practice}, Report 108 (2008) vol 1, 322–3.
\item[149] See, de-identified information does not meet the definition of ‘personal information’; \textit{Privacy Act 1988} (Cth) s 6(1) ‘personal identification’.
\item[150] Ibid sch 1 pt 2 sub–cl 3.3(a)(i).
\item[151] Ibid s 6FB ‘health service’.
\item[152] Ibid s 6FA(b) ‘health information’.
\end{enumerate}
\end{footnotesize}
and does not, under the Privacy Act, require consent for collection or use *even if obtained during the provision of a* ‘health service’.

For example, a clinical image of skin, 2 x 2 cm², taken during a consultation as an aid to diagnosis and which has been de-identified *does not require consent, under the Privacy Act*. The Act does not prevent it from being shown to colleagues, displayed at conferences, or published on websites or in textbooks.

The *Health Practitioner Regulation National Law Act 2009* (the ‘National Law’)¹⁵³ and the Medical Board’s Code¹⁵⁴ both place more stringent consent obligations upon the medical practitioner. These will be discussed in more detail in Chapter V, ‘Regulatory Bodies and Codes of Conduct’. It is relevant to observe here that in these legislation and regulations the *circumstances* of collecting the photograph, rather than the identifiability of the subject individual, determine the obligation for consent. For almost all clinical photographs, consent, under these obligations, is required. A practitioner who contravenes the Code is open to regulator sanctions; however, this does not provide any restitution for the affected individual.¹⁵⁵

Patient consent may be *express*, written or verbal, or *implied* by conduct.¹⁵⁶ Voluntarily posing for the photograph may be regarded by the practitioner as ‘implied consent’.¹⁵⁷ Patients, however, may interpret their actions and the boundaries of their consent differently.¹⁵⁸ Ian Berle, the Royal London Hospital’s medical photographer, explains that some patients expect that photographs taken will only be used for inclusion in the medical records.¹⁵⁹ It might not be clear to the patient that an electronic medical record may be shared and available to all with legitimate access. Consent may also be needed for other uses, such as transmission to

---

¹⁵³ Each state and territory has adopted the *Health Practitioner Regulation National Law Act 2009*, save NSW who has partially adopted the law. This is discussed in detail in Ch 5 ‘Regulatory Bodies’.

¹⁵⁴ Medical Board of Australia, above n 26.


¹⁵⁸ Hood, Hope and Dove, above n 23, 1010.

¹⁵⁹ Berle, above n 47, 89.
colleagues for advice or discussion, education, presentation in clinical meetings or publication in journals or books. 160

In Australia, the Privacy Act permits a practitioner to use and disclose patient photographs for a ‘directly related secondary purpose’ provided it is within a patient’s reasonable expectations,161 such as obtaining expert advice. Indirect use of a clinical image may need additional express consent.162 Doctors may not fully understand this.163 ‘Consent to photography should be discussed on three levels’: medical records, teaching and publication.164 ‘[B]lacking out the eyes and face rarely achieves anonymity’.165 ‘[I]t may be preferable to gain proper and full consent’ for unedited publication of the photograph. 166

Is implied consent actually consensual? The power gradient in the doctor-patient relationship places the patient at a disadvantage.167 Patients might believe that withholding consent may compromise the quality of care they hope to receive.168 ‘[P]assive coercion’ may exist if the medical practitioner does not explicitly offer the patient an unqualified choice to refuse.169

Ideally, written consent should be obtained before taking clinical photographs,170 though verbal consent is more convenient.171 Smartphone cameras enable a quick and less structured approach to documentation.172 This facility may explain why appropriate consent is not always obtained or recorded.173 Comprehensive, contemporaneous recordkeeping is, by the Medical Board of Australia’s Code,174 if not the Privacy Act, considered ‘good [medical] practice’.175
An AMA guide presents an illustrative case in which a patient’s injuries from domestic violence were photographed by the attendant hospital doctor who failed to upload the images to the medical records. A ‘court required [the photographs] production’ in response to a subpoena ‘on the basis that they formed part of the patient’s records’.  

This kind of case reveals both the value and risk of clinical photographs. They allow more accurate and comprehensive documentation but, by becoming part of the medical record, must be retained and secured for at least seven years. During this period, they must remain accessible to the patient, if requested, under the Freedom of Information legislation and APP 12.

Express consent is required by the Privacy Act, prior to use or disclosure of ‘sensitive information’ for any purpose not relating directly to the primary purpose. An identifiable photograph taken for clinical diagnosis or documentation, therefore, may not be used for education or publication without prior express consent.

The Code requires ‘obtaining informed consent or other valid authority before … [undertaking] any examination, investigation or provide treatment’. Unlike the Privacy Act, the Code also requires that even non-identifiable pictures are subject to prior consent for each and every use. MDA National, an Australian medical indemnity insurer, reinforces this view: ‘the patient’s consent must nevertheless be sought prior to the taking of any photographs or films’ even if the ‘patient cannot be

---

176 Australian Medical Association, above n 79.
178 In most cases this is a 7 year period; see, eg, Mahar et al, above n 17, 48; Australian Medical Association, above n 79.
179 Mahar et al, above n 17, 48.
180 Freedom of Information Act 1982 (Cth); Kirk et al, above n 23, 41.
181 Privacy Act 1988 (Cth) sch 1 pt 5 sub–cl 12.1.
182 Privacy Act (Cth) sch 1 pt 3 sub–cl 6.1(a).
183 Medical Board of Australia, above n 26.
184 Ibid.
identified in [the] photograph’. Consent should be ‘clearly documented and the scope of any such consent be recorded.’

Clearly defined written consent can prevent future disputes. This was seen in the US case of Anderson v Mayo Clinic. The patient, Anderson, gave the Mayo Clinic full written consent to use her health information, including videos and photographs, in any way the Mayo Clinic saw fit. Anderson did not expect the hospital to allow her images to be broadcast on local TV. Her written consent, which included the Clinic’s use of her images, prevented her privacy suit from succeeding.

Inadequate documentation of consent leaves health providers vulnerable. A Dr Valentine, in a 2006 UK case, failed to record verbal consent from patients on 13 separate occasions. The ‘General Medical Council’ (UK) (‘GMC’) reproached Dr Valentine for careless record keeping and cautioned against failing to adhere to professional standards of practices. Documentation of consent for all forms of use and disclosure might protect the practitioner from future medico-legal jeopardy.

C The Issue of Identifiability

Clinical photographs enrich public awareness, facilitate research and can be invaluable clinical resources. Using them for these purposes are secondary to the primary purpose under the Privacy Act and the Code; identifiable images may only be used if the patient grants consent. Consent is more readily given by patients for de-identified photographs to be used for secondary purposes. This was overwhelmingly supported by hand surgery patients.

187 Ibid.
188 Anderson v Mayo Clinic, 2008 WL 3836744 (Minn. App.)
191 Taylor et al, above n 70, 39; Baldwin, above n 186, 4; Cunniff et al, above n 2, 353.
192 Cesar Palacios-Gonzalez, ‘The Ethics of Clinical Photography and Social Media’ 2015 18 Medical Health Care and Philosophy 63, 64.
193 The ‘primary purpose’ is the purpose that the collection was made (e.g. taking the photograph); see Privacy Act 1988 (Cth) sch 1 pt 3 sub–cls 6.1–6.2; Medical Board of Australia, above n 26.
194 Privacy Act 1988 (Cth) sch 1 pt 3 cl 6.
195 Lau, Schumacher and Irwin, above n 61, e508.
196 Jillian Tomlinson, Andrew Myers and Bryce Mead, ‘“Click First, Care Second” Photography: To the Editor’ 2013 198(1) Medical Journal of Australia 21, 22.
Sometimes, the inclusion of identifying characteristics is unavoidable. As mentioned above, anatomical features, such as an ear or lip may serve as a landmark reference or, for example, a rash may cover a large body part, such as the side of the face. Previous methods (e.g. black-boxing and pixelating identifying regions) do not adequately de-identify people. Patient consent for image disclosure for intended uses is preferred, a position which is supported by the International Committee of Medical Journal Editors.

It does, however, raise the question - when applied to the context of clinical photography, when is an image no longer considered ‘reasonably identifiable’? De-identification is not always straightforward. Unique identifiers, such as a patient’s name, address or Medicare or hospital record number must obviously be removed. Is there an element of subjectivity, especially where subtler features are in present? More subtle marks of identity may include distinct jewellery, birthmarks or scars that are inadvertently included in a photo. Unusual anatomical or pathological features may also be identifiable.

In a US case involving the Mayo Clinic, a patient’s genitals, tattooed with the phrase ‘hot rod’, was photographed during gall bladder surgery. When these photographs

197 Lau, Schumacher and Irwin, above n 61, e510; Also see Case 3 example in John B Kelly and Hanspaul S Makkar, ‘Ethics in Pediatric Dermatology’ 2012 30 Clinics in Dermatology 471, 474.
199 June Robinson, Ashish Bhatia and Jeffrey Callen, ‘Protection of Patients’ Right to Privacy in Clinical Photographs, Video, and Detailed Case Descriptions’ 2014 150(1) Journal of the American Medical Association Dermatology 14, 14; Franchitto et al, above n 71, 211; Taylor et al, above n 70, 39.
200 Privacy Act 1988 (Cth) sch 1 pt 3 cl 6.
202 Australian Government, above n 142, 53; The OAIC was encouraged to publish guidelines to assist entities with the Act’s application; Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 53.
204 Berle, above n 47, 43; Berle, above n 47, 89.
205 Stevenson, Finnane and Soyer, above n 4, 198; Mahar et al, above n 17, 49; Kunde, McMeniman and Parker, above n 75, 195.
were leaked to the media, the patient, a male escort, sued the hospital for invasion of privacy. The action was settled out of court.\textsuperscript{207}

Consider, a practitioner seeing a patient, believes a patient photograph she has taken is not ‘reasonably identifiable’ under the Privacy Act. Nevertheless, the patient provided implied consent by posing for the photograph. An image may be shown to an audience, which contains a friend of the patient who is familiar with a tattoo or earring visible in the picture. When combined with the case description, which is likely to include the patient’s age, sex, health or occupational background, might allow that audience member to identify the individual patient. This will be explored later in this Chapter.\textsuperscript{208}

If de-identifying a photo reduces the risk of a privacy breach - at what stage, from patient to record, should de-identification of a photograph occur? If no unmistakable identifier, such as patient name or medical record number, is linked to the captured image, how can filing errors be avoided with certainty? If each image is not uploaded directly into the corresponding patient’s record, the separation in time, location or camera operator exposes the record to mistaken assignment.

GPs practicing in primary care dermatology\textsuperscript{209} may, in one day, consult a considerable number of patients, taking several photographs of each patient. Time constraints do not always allow a practitioner to save patient images to each record contemporaneously.\textsuperscript{210} These circumstances coupled with innate human error leaves even the most conscientious medical practitioner at risk of inadvertently saving an image incorrectly.\textsuperscript{211}

\textsuperscript{207} Segal and Sacopulos, above n 189, 239.
\textsuperscript{208} See Ch III Part F ‘Loss of Control – “Information Drift”’.
\textsuperscript{209} For example the RACGP offers GPs the opportunity to complete a ‘Certificate of Primary Care Dermatology’ for complete details see RACGP, \textit{Certificate of Primary Care Dermatology} <http://www.racgp.org.au/education/courses/dermatology/>.
\textsuperscript{210} Pharmacology and Therapeutics Panel Discussion, above n 115, 00:18:30.
\textsuperscript{211} Ibid 00:18:50.
Patient consent does not relieve the practitioner of the requirement to ensure its inclusion in the medical record or to keep the image securely. The risk of breach is substantially elevated when images are taken on a portable device, e.g. a mobile phone or camera. This workflow is regarded as asynchronous: the photo is not transferred directly to the medical records at the time it is taken. A period of time elapses before it is uploaded to the medical records. The upload may be done via a cable, email and internet, or wirelessly. Store-and-forward telemedicine involves the practice of taking a clinical image with the primary intention of sending it to a third party for advice. Teledermatology is the store-and-forward of images of the skin that are sent to a specialist dermatologist.

Asynchronous workflows expose special hazards to privacy and confidentiality. A clinical photo may not be included in the medical record; it may be left on the portable device, subject to theft, loss, or unauthorised disclosure or it may be insecurely transferred to the medical records or a third party.

The failure to include the photograph into the medical records may be inadvertent: caused by forgetfulness, carelessness, laziness or a technical transmission fault. It may also be deliberate if a clinician decides to redact photographs deemed poor quality, redundant, non-essential, or insufficiently representative.

Excluding clinical photographs from the medical record might be legitimate, but still expose the practitioner to an accusation of destroying part of the clinical record. Metadata, such as date, time and alphanumerical file identifier, is created at the same time as the digital photo. The inclusion into the medical records of image #14 and #16 of a consecutive series but not #15 may need to be defended years later. Regular skin cancer examinations may use photographs to monitor changes. Benign editorial

---

213 Stevenson, Finnane and Soyer, above n 4, 198-200.
214 Ibid.
215 Ibid.
216 Kirk et al, above n 23, 41.
217 Burns and Belton, above n 1, 265; Burns and Belton, above n 138, 439; Kunde, McMeniman and Parker, above n 75, 193.
218 Pharmacology and Therapeutics Panel Discussion, above n 115, 00:24:18.
219 Ibid 00:23:35.
decisions may lead to challenges by patients about the accuracy of the historical record. Gaps in the file sequence may appear suspicious.\textsuperscript{220}

The security risk can be recognised in the following case scenario.\textsuperscript{221} A hospital registrar provides his intern advice after reviewing clinical images emailed to his digital device while having coffee at a public Wi-Fi hotspot. He forgets to delete the images from his device, and, unaware, the images are automatically backed up to his personal online storage, which he shares with his family. Security risks may include every step in the wireless transmission and receipt of the image, the physical safety of his device, the access from unintended family members’ devices. The routines of online behaviour in personal life may camouflage threats to the security of online health information communication and unwitting breach of patient confidentiality and privacy.

In one study, surveyed practitioners retained over 100 photographs (85%).\textsuperscript{222} In another, 74% of doctors retained patient images, of which 32% were identifiable.\textsuperscript{223}

‘Retaining images on mobile phones encourages … showing [them] at a later date. When viewed in a clinical setting the images … provide … clarity of a patient’s condition, but when viewed … during casual conversation in a public venue the same images could constitute a form of entertainment, a practice clearly at odds with ethical conduct’.\textsuperscript{224}

The same behaviour may be ethical in one situation and unethical in another. An altered context may result in a direct breach of Privacy Principle (APP 6) ‘use and disclosure’ leading to heavy individual and organisational penalties.\textsuperscript{225}

\textsuperscript{220} Ibid 00:23:49.
\textsuperscript{221} Australian Medical Association, above n 79.
\textsuperscript{222} Kunde, McMeniman and Parker, above n 75, 193.
\textsuperscript{223} Hubbard, Goodard, and Walker, above n 138, 493.
\textsuperscript{224} Burns and Belton, above n 138, 440; Richard Dean, The Value of Humanity in Kant’s Moral Theory (Oxford University Press, 2006).
\textsuperscript{225} Privacy Act 1988 (Cth) ss 13G, 80W.
E Security Issues of Digital Clinical Photography

The inadequate precautions taken by doctors, to protect the security of clinical photographs is an emerging area of medico-legal risk in Australia. American doctors’ clinical photography use has exposed the vulnerability of portable devices. Weaknesses in portable device protection, cloud storage and back-up control, digital storage and transmission encryption were flagged as security threats. Violations of US federal legislation have already occurred.

In 2012, a digital camera which belonged to the dermatology department of the University of California, San Francisco Medical Centre (‘UCSF-MC’) was stolen from an employee doctor’s locked car while parked at that doctor’s home. The camera’s digital data had not been cleared when it was removed from UCSF-MC and still contained identifiable photographs of patients. UCSF-MC was found responsible for failing to protect patients’ information from unauthorised access. As the stolen camera, like most stand-alone cameras, had no data encryption capability, additional precautions to safeguard the camera from loss or theft should have been taken. UCSF-MC was fined by federal regulators $250,000 and warned of subsequent $2.5 million fines for repeat violations.

In 2012, the Massachusetts Eye and Ear Infirmary and Associates paid $1.5 million for privacy and security breaches when a laptop containing unencrypted patient information was stolen. The Office of Civil Rights (‘OCR’), a regulatory body reminded health providers to ensure encryption of health information stored on all portable devices.

---

226 Baldwin, above n 186, 4.
227 Nielsen, West and Shimizu, above n 20, 2-3; Kunde, McMeniman and Parker, above n 75, 195-6.
229 USD $250,000 is equivalent to approximately AUD $330,000 (Conversion: USD $1 = AUD $1.32)
230 Pharmacology and Therapeutics Panel Discussion, above n 115, 00:17:43.
Clinical photography can be a valuable tool for junior hospital doctors, who are more likely to need frequent diagnostic advice.\textsuperscript{232} The use of smartphones for clinical photography is most common in the same cohort.\textsuperscript{233} Smartphones facilitate seamless communication between practitioners, offering imaging, storage, and transmission capabilities. This convenience must be balanced with practitioners’ obligations to reasonably protect patients’ photographs from ‘interference, misuse and loss, unauthorised access, modification or disclosure’.\textsuperscript{234} Unencrypted clinical photos sent through publically accessible Wi-Fi internet may compromise security. Doctors who rely on the minimal precautions they apply to storing or uploading personal photos jeopardise patient privacy and confidentiality. Reception by a recipient at home or on a portable device incurs similar risks. Once the image is transmitted, the sender has lost control unless the entire transmission is within satisfactory security standards.\textsuperscript{235}

Two influential groups, the Australian Medical Association and Medical Indemnity Industry Association of Australia (‘MIIAA’) recommend that practitioners delete images from the recording device as soon as they have been transferred into the patient’s medical record.\textsuperscript{236} Unlike stand-alone digital camera, people carry their phones with them, heightening the susceptibility to loss, theft and unauthorised access.\textsuperscript{237} Regularly deleting clinical images from the phone once uploaded to the patient’s file is an effective way to mitigate the risk of a privacy breach,\textsuperscript{238} yet as cited earlier, studies indicate practitioners are not heeding these warnings. Interestingly, even simple security precautions are not being taken. One survey showed only 23\% of practitioners had security passwords on devices used for clinical photography,\textsuperscript{239} another reported less than 50\% used passwords on their phones.\textsuperscript{240} This is despite the AMA’s recommendation that passwords be used on mobile phones containing clinical photographs to prevent unauthorised access.\textsuperscript{241}

\textsuperscript{232} Jamil, above n 112, 105.
\textsuperscript{233} Nielson, West and Shimizu, above n 20, 2.
\textsuperscript{234} Privacy Act 1988 (Cth) sch 1 pt 4 sub–cl 11.1.
\textsuperscript{235} Nielson, West and Shimizu, above n 20, 1; Luo et al, ‘Cyberdermatooethics I: Ethical, Legal, Technologic, and Clinical Aspects of Patient-Physician e-mail’ 2009 27Clinics in Dermatology 359, 360-1.
\textsuperscript{236} Australian Medical Association, above n 79.
\textsuperscript{237} Nielson, West and Shimizu, above n 20, 2.
\textsuperscript{238} Davis, above n 73, 119.
\textsuperscript{239} Kunde, McMeniman and Parker, above n 75, 193.
\textsuperscript{240} Kirk et al, above n 23, 42.
\textsuperscript{241} Australian Medical Association, above n 79.
Added to this legal quagmire are the everyday occurrences of automatic cloud storage back ups and auto-synchronisation across multiple devices. These overtly routine functions add to the mounting security challenges. When clinical photographs are uploaded to the cloud, disclosure has occurred; if it is an overseas cloud provider, APP 8 governing ‘cross board disclosure’ is invoked. Prior to disclosing any patient information (clinical photographs), APP 8.1 requires the disclosing entity (the practitioner) to take ‘reasonable steps’ to ensure the storage provider is APP compliant. Failing this, the disclosing entity (the practitioner) can be held accountable, under s 16C of the Privacy Act, for any third party breach (e.g. if a practitioner’s cloud provider was hacked). Should mandatory data breach reporting become law, the disclosing party would be responsible for reporting an overseas breach.

In contrast to hospital-based doctors, most GPs work inside an office, an enclosed private space within a group practice using a dedicated desktop computer through which they access patient records residing in digital files on a server located in the same building (and certainly within close proximity) as their office. Unless the GP participates in ownership or management of the whole practice, IT security is usually assumed by the GP to be adequate and safe. GP practice owners often delegate IT security, maintenance and service to a third party vendor. Individual practitioners, faced with a busy work schedule and a working computer have little motivation to consider the security of their computers, servers, or internet feed. Brought from home, and part of their own personal lives, their smartphones with cameras, portable laptops or storage devices (e.g. USB thumb drives) trigger even less concern or caution. As far as they are aware, patient records are physically secure and backed-up. It is unlikely that many doctors have ever needed to retrieve  

242 Nielson, West and Shimizu, above n 20, 1-2.  
244 Davis, above n 73, 118; Kirk et al, above n 23, 41.  
245 Privacy Act 1988 (Cth) sch 1 pt 3 sub-cl 8.1.  
246 Ibid sch 1 pt 3 cl 8.  
247 Pharmacology and Therapeutics Panel Discussion, above n 115, 00:19:04.  
248 Explanatory Memorandum, Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Cth) 19-20.
data files that have been corrupted or otherwise rendered inaccessible. Fewer still contemplate data theft, intentional corruption or incompetent data integrity. The majority of general practitioners are not aware of risk management practices and procedures for clinical photography, in particular, images that are captured on personal smartphones.

The literature makes a compelling case for the divergence between actual practices of hospital-based doctors and their legal and professional obligations. It is likely that the same complacency and ignorance of obligation and risk that exists in hospital-based doctors is at least as prevalent among GPs who work alone, or even in group practices, within a reassuringly familiar environment and run by staff with whom they have a long-standing acquaintance and comfort.

Many medical practitioners are not aware that clinical photographs are a part of the patient’s medical record from the moment the photograph was taken, rather than later, when it is uploaded into the patient’s Electronic Medical Record (‘EMR’). It is even less likely, then, that GPs will equate the obligations of privacy and confidentiality that attach to the EMR with the same obligations of the clinical photograph after it has been taken. Similar problems arise with consent for different uses of clinical photographs.

Hospital doctors live daily with a certain amount of protocol and bureaucracy, and so have a lower threshold for recognising when the possibility for breach of protocol has occurred. The multi-user nature of hospital medical records encourages the clinical photographer, whether a dedicated photographic professional or a practitioner with a camera, to upload photos as soon as they are taken, especially if the photograph will facilitate another doctor’s guidance in diagnosing or managing a patient. GPs who seek specialist advice have little alternative but to send a clinical photograph externally, by email or other means (cloud storage, etc.).

---

249 Collection of personal information; Privacy Act 1988 (Cth) sch 1 pt 3 cl 3.
250 For example, GPs using teledermatology will request a remote consult by providing the dermatologist with digital images of patients’ skin conditions through the store and forward method; van der Heijden et al, ‘Teledermatology Applied Following Patient Selection by General Practitioners in Daily Practice Improves Efficiency and Quality of Care at Lower Cost’ 2011 165 British Association of Dermatologists 1058, 1058.
Unlike the US there have been no Australian cases to date involving clinical photography that have attracted a comparable regulatory fine, however, APP 11 states that APP entities251 (including all private health service providers) are expected to take ‘reasonable steps’ to protect personal information from ‘misuse, interference, loss, unauthorised access, modification and disclosure’.252 ‘Reasonableness’ is determined by circumstances and context. Reasonable steps to protect information will depend on the sensitivity of the information and the risk of harm that would be caused by a breach.253 If the information is sensitive and the risk of harm is great, higher security measures would be expected for storage, access and transmission of information.254 If the proposed Privacy Amendment Bill is passed, reporting will become mandatory, alerting the Privacy Commissioner and the affected parties.255 This is likely to raise the profile of privacy breaches and any negative consequences, as has been demonstrated in the US.256

F  Loss of Control – ‘Information Drift’

 Appropriately shared digital data may still lead to unauthorised dissemination. ‘Store and forward’257 image transfer risks ‘drift’258 beyond an authorised use and context. Smartphones are familiar, easy to use, immediately accessible, and can take quality images.

Consider: A photographed hand rash, taken for documentation in the medical record (‘the primary purpose’)259 is sent from the GP to a dermatologist for advice (a directly related secondary purpose, according to the Privacy Act.)260

251 See Privacy Act 1988 (Cth) s 6(1) (entity, organisation and corporation are collectively referred to as ‘APP entities’).
254 Ibid.
255 Note: Currently Australian Privacy Principle 11 mandates Data Breach Notification but only requires APP entities to take ‘reasonable steps’ to protect personal information; Privacy Act 1988 (Cth) sch 1 pt 4 cl 11.
256 Guffin, above n 36, 6-12.
257 ‘Store and forward’ is where the original party retains a copy of the information, for example, a photograph, then electronically transmits a copy to another party. This process, if repeated countless times by multiple receivers, poses a real and present risk to privacy through unauthorised dissemination.
258 Lenardis, Solomon and Leung, above n 11, 588.
259 Privacy Act 1988 (Cth) sch 1 pt 2 cl 3.
260 Serious interference with privacy and a breach of confidentiality; Privacy Act 1988 (Cth) sch 1 pt 3 sub–cl 6.2; Office of the Australian Information Commissioner, above n 243.
The dermatologist, after diagnosing secondary syphilis, uses the photo for a seminar with registrars. An unusual engagement ring, visible in the image, is recognised by one registrar who can now identify the patient with whom she is acquainted. The patient, a beneficiary of the dermatologist’s remote diagnosis, may be unaware of her involvement. There has been ‘drift’ from the primary purpose of collection under APP 3, to an unrelated secondary purpose of disclosure under APP 6, the education of trainees. This would be a serious ethical and legal breach of both the Privacy Act and the Code. Express consent was never formally obtained. Voluntarily posing her hand, the patient’s implied consent would not also cover the use and disclosure of parts of her health information for educational purposes. An individual, may, at any time, withdraw consent. Dissemination of the image as just described, let alone if published online or in a textbook, may be irretrievably lost to unauthorised circulation.

G The Effects of Social Media on Attitudes Towards Privacy

Social media, such as Facebook, Instagram, Snapchat and Twitter, is used daily by millions of users worldwide who share personal information and connect with other users. Accepted by all generations, but especially the younger ones, social media provides a connection with family and friends and a bridge to new relationships. What began as personal networks has been avidly embraced by businesses to market identity, products and services. To gain the many benefits user voluntarily sacrificed some control over the privacy.

According to Statista, an international statistics company, more than two-thirds of US internet users in 2016 were social media users. Facebook had 15 million

---

261 See Privacy Act 1988 (Cth) ss 13G, 80W; Medical Board of Australia, above n 26.
262 ‘Education and publishing’ are secondary purposes to the primary purpose (recording and diagnosis the condition) for which the information was collected; Privacy Act 1988 (Cth) sch 1 pt 3 sub–cl 6.2(a).
263 Palacios-Gonzalez, above n 192, 68.
264 Kristen A Carruth and Harvey J Ginsburg, ‘Social Networking and Privacy Attitudes Among College Students’ 2014 6(2) Psychology, Education & Society 82, 83.
265 Ibid.
266 Sánchez Abril, Levin and Del Riego, above n 7, 66.
unique Australian visitors to its site during October 2016\textsuperscript{268} out of an estimated resident population of 24 million.\textsuperscript{269} Of especial relevance, social media is accessed in the US via smart phones 67\% of the time, and portable devices over 80\% of the time.\textsuperscript{270} There is no reason to believe Australian habits are different.

Professional and personal lives involve ‘boundary-crossing technology’ that is social media.\textsuperscript{271} Fortunately for the medical profession, where patients’ privacy and confidentiality are concerned, traditional boundaries separating a practitioner’s professional and personal life are clear.\textsuperscript{272} Despite these boundaries inappropriate posts on social media sites have been made by many medical students.\textsuperscript{273} Of the medical colleges surveyed by Chretien et al, 60\% disclosed instances involving unprofessional or inappropriate posts, of which 13\% had breached patient privacy.\textsuperscript{274} ‘[U]nidentified’ patient information was posted by medical students unaware their posts gave sufficient detail to violate patient privacy.\textsuperscript{275} In Rhode Island, US, an Emergency Department doctor, Alexandra Thran, M.D., posted a description of an unnamed patient’s injuries, sufficiently detailed to permit identification by third parties of the individual. The doctor was reprimanded and fined by the State Medical Board though not found guilty of unprofessional conduct.\textsuperscript{276} She was fortunate. Social network user profiles often contain details of their profession and work affiliation. These details may contribute to inadvertent patient identification, privacy and confidentiality breaches.\textsuperscript{277}

The AMA’s ‘Clinical Images Guide’\textsuperscript{278} provides a case study, “\textit{Guess what happened at work today?}”, to illustrate the hidden risks to patient privacy and confidentiality of doctors using social media. Witnessing a cardiac arrest during surgery:


\textsuperscript{270} Statista: The Statistics Portal, above n 267.

\textsuperscript{271} Sánchez Abril, Levin and Del Riego, above n 7, 66.

\textsuperscript{272} See APP 6 - Use and disclosure: \textit{Privacy Act 1988} (Cth) sch 1 pt 3 sub–cl 6.

\textsuperscript{273} Chretien et al, ‘Online Posting of Unprofessional Content by Medical Students’ 2009 302(12) \textit{Journal of the American Medical Association} 1309, 1309, 1312.

\textsuperscript{274} Ibid 1309, 1312.

\textsuperscript{275} Ibid 1312, 1314.

\textsuperscript{276} Simrall, above n 231.

\textsuperscript{277} Ibid.

\textsuperscript{278} Australian Medical Association, above n 79.
‘A medical student filmed the resuscitation on her iPhone, and posted the footage on Facebook. Although the patient was not identifiable, the student tagged the name of the hospital in her status, “Guess what happened at work today?”’279

The younger generation have grown up in an age of ever-advancing technology.280 Continuous online peer communication and social interactions have shaped not only their social mores but also their understanding of how reality is revealed.281 It is ‘informal and fast paced’, an intimate and unfiltered portal into a life, 282 an unending direct cinema that shares daily experiences with a broadband audience. Unlikely in a paper format of restricted distribution, this behaviour may have contributed to an increase in unprofessional and inappropriate online posts.283 Sharing details of personal workday experiences on social media is a norm in which the younger generation are fully immersed. It is based on putting the ‘reporter’ at the centre of the event: it is their experience.284 It may also reflect a finding of the 2008 ALRC report that this generation’s disregard for personal privacy may extend to health information privacy.285 By failing to recognise their privileged position with respect to a patient-provider interaction, junior medical professionals may unwittingly betray patient privacy.

279 Australian Medical Association, above n 79.
280 Sánchez Abril, Levin and Del Riego, above n 7, 96.
282 Carruth and Ginsburg, above n 264, 83.
283 Australian Medical Association, above n 79.
IV REGULATORY BODIES AND CODES OF CONDUCT

A The Introduction of the Modern Professional Code

The first modern code of medical ethics, a term the author may have been the first to use, was published in 1803 by Thomas Percival. It sought to provide a code of conduct of physicians in four areas: within hospitals, in private and general practice, in relationships with apothecaries (who traded in both medical advice and therapeutic compounds), and in those duties that required knowledge of the law. ‘Secrecy, and delicacy when required by peculiar circumstances, should be strictly observed’. It was a physician-centric code, relying on the ‘scrupulous regard [of the physician] to fidelity and honour… [and] …of professional conduct in private or general practice’. It was a gentleman’s code of practice for members of a prestigious ‘guild’ to practice in recognition of their mutual respect. It would be adapted, over time, to become the foundation of many medical ethics codes worldwide.

Drawing from the principles of Percival’s work, the second General Assembly of the World Medical Association (‘WMA’) adopted, in 1948, the Declaration of Geneva, also known as the ‘Physician’s Oath’. The Oath was a commitment to human rights within medicine. It was developed, in part, as a response to participation of doctors in Aktion T4, the Nazi involuntary euthanasia program and in medical atrocities in concentration camps, which led to their prosecution in the Nuremberg Doctors’ Trials. The Oath vowed ‘respect for human life’, a prohibition against using ‘medical knowledge [used] to violate human rights and civil liberties’ and to ‘…RESPECT [sic] the secrets that are confided in me, even after the patient has died’.

286 Higgins, above n 87, 922.
287 Thomas Percival, Medical Ethics: or, a Code of Institutes and Precepts, Adapted to the Professional Conduct of Physicians and Surgeons (London: W Jackson, 1803) 390.
288 Ibid.
289 Higgins, above n 87, 923.
290 In August 1947, twenty Nazi physicians and three medical administrators stood trial for ‘murders, tortures and other atrocities’ whereby medical experiments were performed on ‘unwilling victims’. The Nuremberg Tribunal found sixteen of the defendants guilty and sentenced the defendants to either extended prison sentences or death by hanging; Albert Jonsen, Short History of Medical Ethics (Oxford University Press, 2000) 100.
Society had already begun to identify, if not incontrovertibly define, a right to privacy. This would be pivotal in the foundational legal article, ‘The Right to Privacy’\(^{292}\) in which Warren and Brandeis J\(^{293}\) argued the evolution of a right of protection ‘to be let alone’.\(^{294}\) They recognised the role that rapid dissemination of information, in the form of mass media and the unauthorised photograph, could have on the destruction of privacy. Brandeis presciently anticipated the day of intrusive technology when he wrote ‘numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.”’\(^{295}\) The forces were forming that would unite human rights and privacy...

With this movement towards placing the individual as the cardinal actor in decisions that affected mind and body, medical codes were transformed to a patient-based right;\(^{296}\) the underlying principle was a belief in the ‘human right’ to autonomy.\(^{297}\) Contemporary medical professional codes no longer depended on a physician’s paternalistic determination of legitimate distribution of patient information. Codes were built upon patient privacy, autonomy and right to confidentiality.

B  The Role of Professional Codes in Healthcare Regulation

Regulation of the medical profession began in England under the reign of King Henry VIII, in 1511\(^{298}\) to help ensure that only those suitably qualified and competent were able practice.\(^{299}\) The goal of regulation was primarily public safety; to protect the sick, weak and vulnerable from charlatans and quackery.\(^{300}\) A formal ‘medical register’ of licensed practitioners was not established until the creation of the ‘General Council of Medical Education’ under the Medical Act 1858 (UK). Practitioners guilty of inappropriate conduct could be deregistered, barring them from legally practicing medicine.\(^{301}\)

---

293 Louis Brandeis J was a US Supreme Court Justice from 1916–1939.
294 Warren and Brandeis, above n 292, 193.
295 Ibid 195.
296 Higgins, above n 87, 922.
297 Secretary, Department of Health and Community Services (NT) v JWB (Marion’s case) (1992) 175 CLR 218; Amaboo and Payne-James, above n 41, 59–60.
298 Allan and Blake, above n 30, 562.
299 Ibid.
300 White, McDonald and Willmott, above n 63, 617.
301 Allan and Blake, above n 30, 563.
Australian states had already begun to enact medical regulatory legislation: first NSW in 1838 \(^{302}\) and, unusually, Western Australia was next in 1869.\(^{303}\) Regulatory and accreditation standards differed by state and territory.\(^{304}\) Practitioners registered in one state wishing to practice in another state were required to formally apply to register with that state’s medical board. Medicine, unlike law, does not significantly change across state borders. Eventually, the ‘National Registration and Accreditation Scheme’ (the ‘NRAS’) was introduced on 1 July 2010 and was adopted by all states and territories. NSW, however, did not adopt the NRAS in full, refusing to cede control of its medical complaints system.\(^{305}\)

The NRAS allowed unification of Australian medical registration and accreditation standards.\(^{306}\) The scheme is governed by the ‘Australian Health Practitioner Regulation Agency’ (‘AHPRA’), which, in turn, supports fourteen National Health Practitioner Boards.\(^{307}\) One of these boards, the Medical Board of Australia (‘MBA’), became responsible for regulating Australian medical practitioners.\(^{308}\) Other boards regulate other health practitioners, such as dentists, physiotherapists, pharmacists or psychologists.\(^{309}\)

The Australian medical profession has embraced ethical codes. Regulatory bodies, such as the Medical Board of Australia, which administers medical practitioner registration on behalf of AHPRA, makes conformity with its professional ‘Code of Conduct’\(^{310}\) a requirement of registration.\(^{311}\)

Breaches by doctors of the MBA Code,\(^{312}\) however, do not afford patients any legal rights of privacy. Such breaches, including those, which involve patient confidentiality, are dealt with directly through regulatory sanction imposed directly

---

\(^{302}\) ‘An Act to define the qualifications of Medical Witnesses at Coroners’ Inquests and Inquires held before Justices of the Peace in the Colony of New South Wales 1883 (NSW) (2 Victoria, Act No 22)’ cited in Allan and Blake, above n 30, 569.

\(^{303}\) Medical Ordinance Act 1869 (WA) as cited by Allan and Blake, above n 30, 569.

\(^{304}\) Allan and Blake, above n 30, 578.

\(^{305}\) Ibid 578.

\(^{306}\) Ibid 578-9.

\(^{307}\) See Annexure A for complete list of National Boards.

\(^{308}\) Medical Board of Australia, About &lt;http://www.medicalboard.gov.au/About.aspx&gt;.


\(^{310}\) ‘Code of Conduct’ is the contemporary term, replacing ‘oath’, ‘declaration’ and ‘ethical code’.

\(^{311}\) Allan and Blake, above n 30, 561.

\(^{312}\) Medical Board of Australia, above n 26.
upon the offending doctor. Sanctions may be enforced by either or both the MBA\textsuperscript{313} and the Privacy Commissioner under the relevant provisions of the Privacy Act.

Individual specialist medical colleges, such as the Royal Australian College of General Practitioners (‘RACGP’), set the standards for education, training and quality of medical practice. The RACGP, for example, does not have an enforceable code of conduct, but reminds its members by reference to their obligations under the MBA’s Code and federal and state privacy laws.

Trade bodies, such as the AMA, the Rural Doctors Association of Australia and the Doctors Reform Society, exist to identify and promote policies favourable to their membership. These organisations may also promulgate codes and guidelines, though without force of law or obligation.\textsuperscript{314}

\section*{C Confidentiality and Professional Codes}

Both patients and society\textsuperscript{315} assume that their doctors will not divulge personal or health information.\textsuperscript{316} Medical ethics have evolved since the advent of the Hippocratic Oath, however confidentiality remains a core element. Breach of confidentiality is considered ‘unprofessional conduct’ and subject to sanction.\textsuperscript{317}

The right to confidentiality is not absolute. It may be forced to yield by legal compulsion; mandatory reporting of certain communicable diseases,\textsuperscript{318} court-sanctioned evidential enquiry\textsuperscript{319} and where law or necessity deems that public

\begin{thebibliography}{10}
\bibitem{313} Health Practitioner Regulation National Law (WA) Act 2010 (WA) sch pt 5 s 40; Ian Kerridge, Lowe and McPhee, above n 38, 229.
\bibitem{315} Richard Cruess and Sylvia Cruess, ‘Updating the Hippocratic Oath to Include Medicine’s Social Contract’ 2014 48 Medical Education 95, 96.
\bibitem{316} Kim Forrester and Debra Griffiths, Essentials of Law for Medical Practitioners (Churchill Livingstone Elsevier Australia, 2011) 65.
\bibitem{319} Brown v Brooks (Unreported, Supreme Court of New South Wales, McLelland J, 18 August 1988).
\end{thebibliography}
interests, such a threat from imminent harm, outweigh respect for individual privacy. Consent, a concept that is inextricably linked to privacy and confidentiality, is also addressed in the MBA code. It establishes a controlling condition upon the collection of health information from a patient. It is vital to the practitioner-patient relationship. In most circumstances in Australia, medical practitioners must first obtain a patient’s consent before disclosing confidential patient information. Consent ensures that patient autonomy is respected. Patients retain control over how their information is used or disclosed. The duty to obtain consent is not only regulated by the MBA code, but is also enshrined in federal privacy law. Through AHPRA’s delegation to the Medical Board the power to administer the medical register enables the Board to determine the status of individual’s registration. Failure to comply with its Code may result in sanctions, including practice restrictions to full de-registration. There exist other ‘professional’ bodies, such as the RACGP, which support the MBA’s Code.

The following sections provide a brief overview of the relevant Australian regulatory landscape that underpins the obligations of medical practitioners to confidentiality and privacy.

---

320 *W v Edgell* [1990] 1 All ER 855; McIlwraith and Madden, above n 39, 289; Kunde, McMeniman and Parker, above n 75, 195; for a case of imminent harm see, eg, *Tarasoff v The Regents of the University of California* 551 P2d 334 (Cal 1976).
321 Medical Board of Australia, above n 26.
322 Ibid.
323 Allan and Blake, above n 30, 303.
324 The MBA Code is empowered by the *Health Practitioner Regulation National Law Act 2010* (WA) sch pt 5 ss 39–41.
325 *Privacy Act 1988* (Cth) sch 1 pt 3 cl 6; note: there are some differences as discussed in this paper.
The Australian health profession is governed by the \textit{Health Practitioner Regulation National Law Act 2009} (the ‘National Law’). Introduced on July 1, 2010, the National Law has been adopted by, and is in force, in each Australian state and territory, except NSW,\(^{328}\) which chose to retain oversight of its individual health practitioner complaint process. In doing so, NSW does not participate in the national notification system.\(^{329}\) The National Law enables all health practitioners to be registered under a national registration and accreditation scheme,\(^{330}\) so as to ensure nationally consistent standards, assist administrative efficiency and allow only currently registered doctors to practice Australia-wide.\(^{331}\) Special provisions within the National Law renders the Privacy Act binding on all health practitioners registered under the \textit{National Registration and Accreditation Scheme}.\(^{332}\)

The Australian Health Practitioner Regulation Agency (‘AHPRA’) is responsible for providing support to 14 National Boards who are part of the scheme,\(^{333}\) including the Medical Board of Australia. Part of AHPRA’s role is to support health practitioners by developing policies that assist in the provision of healthcare in a safe and appropriate manner. In March 2014 AHPRA published the ‘Social Media Policy’, a ‘National Board Policy for Registered Health Practitioners’,\(^{334}\) which includes a reminder of obligatory professional board codes and the National Law. The policy cautions health practitioners against participating in social media in any way that might contravene patient privacy and confidentiality.\(^{335}\) It warns against social media posts that include unauthorised patient photographs (irrespective of the social media privacy setting) as a clear and direct breach of patient privacy and confidentiality and ‘standards of professional conduct’.\(^{336}\) The policy makes no exception for postings of de-identified clinical photographs.

\begin{footnotes}
\footnote{Allan and Blake, above n 30, 578.} \footnote{Ibid 578.}
\footnote{\textit{Health Practitioner Regulation National Law (WA) Act 2010} (WA) sch pt 1 s 3.}
\footnote{Allan and Blake, above n 30, 578.}
\footnote{\textit{Health Practitioner Regulation National Law (WA) Act 2010} (WA) s 213(1).}
\footnote{See Annexure A for full list of National Boards.}
\footnote{Ibid.}
\end{footnotes}
The National Law empowers the relevant National Boards (for example the Medical Board, Optometry Board or Dental Board) to refer complaints or concerns about a practitioner to a panel hearing which is overseen by AHPRA. The panel is drawn from an approved pool of suitably qualified members of the health profession and the community. The panel helps set professional standards and deals with allegations of misconduct and inappropriate or inadequate performance. Between June 2013 and April 2015, seven medical practitioners have appeared before an AHPRA panel for confidentiality related matters. Complaints about six of the seven related to concerns about inappropriate disclosure, and the seventh alleged inappropriate collection and use of confidential information. Of the seven practitioners, four were held responsible for unprofessional conduct, and one for unsatisfactory professional conduct. All five were cautioned. The remaining two practitioners were found to have no case to answer.

E  The Medical Board of Australia (MBA)

The Medical Board of Australia (‘MBA’) is responsible, by AHPRA’s delegation, for the oversight of Australian medical practitioners. It maintains the medical register and sets the mandatory Code of Conduct. AHPRA is also responsible for the establishment of continuous professional development training and accreditation standards. This role is usually assigned by AHPRA to the individual specialist medical boards, which are maintained by specialty colleges, such as the Royal Australian College of Dermatology (‘RACD’), the Royal Australian College of Surgery (‘RACS’) and the Royal Australian College of General Practitioners (‘RACGP’).

All medical practitioners, regardless of their specialty affiliation, are required to follow the principles prepared by the MBA as set out in ‘Good Medical Practice: A Code of Conduct for Doctors in Australia’ (the ‘Code’). The code embodies core values contained within World Medical Association’s Declaration of Geneva and the

337 Ibid.
339 Ibid.
340 Medical Board of Australia, above n 26.
International Code of Medical Ethics. A serious departure from, or repeated failures to comply with, the Medical Board’s code may affect a medical practitioner’s medical registration. Action may be taken by the MBA that temporarily or permanently restricts or prevents a doctor from practicing medicine within Australia.

Section 3.4 of the Medical Board’s code deals with confidentiality; patients have a ‘right’ to expect that medical practitioners (and staff) will keep patient information confidential. All medical practitioners are expected to abide by applicable privacy legislation, seek informed consent where necessary, and act ethically and legally when using social media. Technology-based consults, such as teledermatology (dermatology at a distance) is explicitly included in the Medical Board’s code.

It is beyond the scope of this paper to address differences in individual state and territory healthcare statutes and regulations. It should be noted, however, that the MBA delegates to the state and territory boards the power to administer practitioner registrations and are each responsible for registration decisions for an applicant seeking to practice in their jurisdiction. A full list of state and territory boards can be found in Annexure B.

F The Royal Australian College of General Practitioners (RACGP)

1 An Overview of the RACGP

Australian medical practitioners who are in training for, or who have completed specialty training in, General Practice may join the Royal Australian College of General Practitioners (‘RACGP’). Founded in 1958 as the ‘Australian College of General Practitioners’ (‘ACGP’) it was granted a Royal Charter a decade later, assuming its current name. Membership, which is voluntary, requires post-graduate obligations. Membership benefits include professional pride, formal

---

341 Ibid.
342 Ibid.
344 A ‘Royal Charter’ is a method of incorporation, i.e. it allows a collection of individuals to be recognised as a body corporate; Privy Council Office, Chartered Bodies <https://privycouncil.independent.gov.uk/royal-charters/chartered-bodies/>.
educational commitments, policy representation and economic incentives provided by the Federal government through access to higher Medicare consultation fees. Like other medical specialist colleges, the RACGP plays dual roles with respect to Australian healthcare regulation: accrediting its specialists, which permit higher Medicare or insurance fees; and advocating policy by lobbying government and the public for changes in national healthcare policy and financing. It has been more successful in the former than the latter role.

2 RACGP ‘Standards for General Practice’

The RACGP has published a ‘Standards of General Practice (4th edition)’ (the ‘Standards’) which ‘provide a template’ to guide general practitioners towards its benchmarks of quality.\(^{346}\) Indicators of compliance with the Standards’ criteria are provided in each section. The Standards reiterate the legal obligations to ensure and maintain privacy and confidentiality, as directed by the Privacy Act and other applicable jurisdictional legislation.\(^{347}\)

Successive editions have increasingly emphasised the role of privacy and confidentiality in electronic medical records and communications in contemporary medical practice. The 5th edition draft was closed for consultation on 30 October 2016, and is scheduled for release on 30 October 2017.\(^{348}\) In the draft, standards for transparency and consent have been strengthened. The current Standards are indicative and somewhat passive: ‘the practice team is aware of how ‘confidentiality of patient health records’ is ensured and patients ‘are informed about [the] policy regarding … management of their personal health information’\(^{349}\) (emphasis added). The draft version of the forthcoming edition is more proactive: ‘patients are informed of how [the] practice manages their confidentiality and personal health information’\(^{350}\) The current edition requires only that the ‘practice team can describe the procedures’ for transferring health information to another provider (emphasis

---

\(^{346}\) Royal College of General Practitioners, above n 32, 2.
\(^{347}\) Royal College of General Practitioners, above n 32, 4.
\(^{349}\) Royal College of General Practitioners, above n 32, 92.
The draft 5th edition permits transfer ‘only after we receive informed patient consent’ (emphasis added). Patients’ health records can be ‘accessed…by an appropriate team member’ will become accessible by ‘only appropriate team members’.

3 RACGP Guidelines – What is Missing?

The College’s Standards publication does address information security, though in sufficiently broad terms to ‘cover the field’. By using this non-specific approach, an inexperienced practitioner using clinical photography, may miss the relevance and application of the guidelines, to clinical photography. Doctors may benefit from a separate publication explaining how best to protect patient privacy and confidentiality by following guidelines tailored to clinical image security. The College publication ‘Handbook for the Management of Health Information in General Practice’ acts as an additional guide, adopting a more practical approach, inclusive of case studies. These publications, though useful, do not address or provide specific guidelines for practitioners engaged in taking clinical photographs. The ‘Standards for General Practices’ states only that the practice ‘must ensure that both active and inactive patient health records are kept safe and securely stored’.

There is no mention that clinical photographs form part of the record.

The College has published a social media guide where it warns against posting patient photographs for privacy reasons while reiterating that the Medical Board’s code applies to social media also. That said, the publication is predominantly directed at how GPs can leverage social media to promote general practice. To date, there is no dedicated College publication addressing the myriad of security related issues that arise from the use of clinical photography. It may be suitable to

---

351 Royal College of General Practitioners, above n 32, 92.
352 RACGP, above n 350.
353 The Royal College of General Practitioners, above n 32, 92.
354 RACGP, above n 350.
355 Royal College of General Practitioners, above n 32, 96-8.
356 Royal College of General Practitioners, above n 156, 4.
357 Royal College of General Practitioners, above n 32, 92-5.
358 Royal College of General Practitioners, Guide for the Use of Social Media in General Practice (2015) 4.
359 Ibid 6-11.
include in this publication, a discussion about the hazards of technology and security, and its impact on patient privacy, followed by recommendations for safer practices.

The RACGP administers the standards for recognition of Vocational Registration (‘VR’), a post-graduate qualification as a specialist general practitioner. Unless and until practitioners achieve this additional qualification, they are by default, Non-Vocationally Registered (Non-VR). The distinction has practical implications for expected standards of practice and for the level of fees rebated by Medicare. This structure may be a powerful motivator for GP College membership. The RACGP has created and maintains its own Continuing Professional Development program (‘CPD’). Interestingly, only one CPD module is consistently required of all doctors, regardless of their specialty status: three-yearly cardiopulmonary resuscitation (‘CPR’). There is, at present, no compulsory requirement for Privacy training. The CPD program may provide a solid platform to introduce a mandatory privacy module.

G The Australian Medical Association (AMA)

The Australian Medical Association (‘AMA’) is a trade group organised to represent the interests of its member medical practitioners, often by creating and disseminating policy position papers or by lobbying government or governmental agencies to favourably consider their proposals. Its role may also be to educate its members about issues that its governing board feels need to be highlighted. Most of its members are not general practitioners, either VR or non-VR, but belong to other specialty colleges. This is partly due to the earnings capability of non-GP specialists relative to GPs, which the AMA, in its role as lobbyist, may do most to influence. The AMA, unlike AHPRA, the Medical Board of Australia and the RACGP, is not a regulatory body.

For example, the RACGP has established the ‘continuing professional development’ (CPD) training program for general practitioners as part of their registration requirements; RACGP, QI&CPD 2014-16 Program <https://www.racgp.org.au/education/qicpd-program/>.

Royal College of General Practitioners, above n 32, 80.

Ibid.

The AMA has published its own code of ethics being a ‘body of ethical principles to guide doctors’ conduct’. The code is based on other widely accepted ethical code, which echo the underlining principles articulated in the Hippocratic Oath. Much like Medical Board’s code, the AMA code promotes the duty of patient confidentiality, accurate contemporaneous record keeping and adequate security of patient information that is stored, accessed and used. Another principle articulated in the code refers to a practitioner’s duty to ensure he or she is apprised of the ‘relevant medical knowledge, codes of practice and legal responsibilities’.

Working with the Medical Indemnity Industry Association of Australia, the AMA released a practical guide for medical practitioners who use digital photography as a clinical tool. Addressed are the numerous perils created when enlisting mobile devices to photograph patients. It is clearly stated that ‘clinical images are ‘health information’ and must be treated with the same privacy and confidentiality as any other health record.’ Straightforward explanations of how to manage clinical photography on mobile devices make it an invaluable resource to the users of this clinical tool. Highlighted are the core issues of privacy and confidentiality, consent, documentation, use and disclosure, de-identification and portability and storage security, and how safe practices can help mitigate the associated risks. Most importantly, the AMA has forewarned practitioners that they risk a substantial fine, in addition to being sanctioned by AHPRA.

The utility of the AMA guide is limited by its restricted distribution. The AMA releases only top-level statistics about its membership. However, by examining and comparing publically available information from the AMA annual report, AHPRA national medical practitioner registration statistics, and RACGP membership statements and estimates, it is reasonable to assume that the AMA officially distributes its guide to less than 10% of specialist GPs. This means that at least

364 Australian Medical Association, above n 327.
365 Ibid.
366 Australian Medical Association, above n 79.
367 Ibid.
368 Ibid.
90% of specialist GPs are not members of the AMA and are unlikely to regularly receive AMA publications and guides. Therefore a helpful guide for which compliance is voluntary, and circulation is very limited cannot be relied upon to improve the standards of practice of clinical photography among GPs.

With Australian privacy legislation for federal, state and territory jurisdictions, application is determined by whether the entity is publically or privately owned and if publically owned, whether it is federally or state / territory owned.

The Privacy Act 1988 (Cth) governs federal public health service providers, along with all private health service providers, including private hospitals. State and territory public health service providers (e.g. state and territory public hospitals) are governed by relevant state and territory privacy legislation, and the federal Privacy Act does not apply.

Where (public) state and private hospitals are co-located, for example, Perth’s Joondalup Health Campus (Joondalup Hospital), applicable legislation is determined by which entity holds the medical record. If it is held by the state public hospital, state legislation applies. Consultant specialists, such as surgeons or anaesthetists, who work in both a public and private role in a co-located hospital or who follow-up their public hospital patients in their private rooms will need to privately hold a copy of the public medical record. Those privately held records are governed concurrently by both state and federal legislation.

Section 3 of the Privacy Act excludes it affecting the operation of state or territory law, although health practitioners, whether they work in a public or private setting, remain subject to all of their obligations under the federal Privacy Act and the APPs.

---

570 As defined by the Privacy Act 1988 (Cth) s 6 (Entity, Organisation, Corporation referred to collectively in the Act as ‘APP entities’)

571 The Privacy Act 1988 (Cth) applies to all health services providers regardless of turnover. The <$3 million turnover exception for private organisations does not apply to health services providers; see s 6D(4)(b). The definition of ‘agency’ includes private corporations; see s 6. The definition of Organisations includes ‘individuals’; see Privacy Act 1988 (Cth) s 6C.

572 Privacy Act 1988 (Cth) s 3.

573 State and territory privacy legislation will not be discussed in this paper. For information on state and territory privacy legislation see: Office of the Australian Information Commissioner, Other Privacy Jurisdictions <https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions>.


575 Privacy Act 1988 (Cth) s 3.
These obligations persist for state-employed doctors because the National Law provides that the Privacy Act applies to all health practitioners registered under the National Registration and Accreditation Scheme (administered by AHPRA).²⁷⁷

A Background of the Privacy Act 1988 (Cth)

The Privacy Act 1988 (Cth) took effect in 1989, regulating how Federal government agencies handle and protect ‘personal information’.²⁷⁸ Enacted under the Australian Constitution’s ‘express power’ with respect to external affairs,²⁷⁹ the Privacy Act fulfilled two key Australian government obligations. It supported the privacy guidelines developed by the Organisation for Economic Cooperation and Development (‘OECD’), of which Australia is a member. It also embraced Article 17 of the International Covenant on Civil and Political Rights, which recognised individual autonomy and privacy as a basic human right by establishing protection of the law for individuals from ‘arbitrary or unlawful interference with his privacy’.²⁸⁰

The OECD ‘Guidelines on the Protection of Privacy and Trans-border Flows or Personal Data’²⁸¹ were designed to facilitate trans-border flow of information between overseas jurisdictions, while ‘protecting privacy and individual liberties’ but furthering ‘economic and social development’.²⁸² They address personal data collection and use; how the data is verified, disclosed and secured. They provide for accountability for errors and breaches and for participation by individuals in maintaining the integrity of their personal data.

³⁷⁶ All states and territories have adopted the National Law (Health Practitioner Regulation National Law Act). Although NSW has only partially adopted the National Law, it participates in the National Registration and Accreditation Scheme, and the Medical Council of NSW has adopted the Medical Board of Australia’s ‘Good Medical Practice: A Code of Conduct for Doctors in Australia’. See Medical Council of NSW for further details.
³⁷⁷ Health Practitioner Regulation National Law (WA) Act 2010 (WA) s 213(1).
³⁷⁸ ‘Personal information’ is defined in the Privacy Act 1988 (Cth) s 6(1).
³⁷⁹ Australian Constitution 1901 (Cth) s 51(xxix); See also Privacy Act 1988 (Cth) Preamble; Rosalind Croucher, ‘President of the Australian Law Reform Commission’ (Speech delivered at the Managing Patient Confidentiality & Information Governance Forum, Melbourne, 22 August 2011).
³⁸² Ibid.
The Privacy Act’s ‘Information Privacy Principles’, based on the OECD Guidelines, applied only to the responsibilities and obligations of government agencies that dealt with personal information. The Privacy Act was amended to cover credit reporting, and then, in 2001, to also regulate the private sector.

The Privacy Act created the role of Privacy Commissioner, first functioning within the Australian Human Rights Commission, and then in 2000 established as an independent Office of the Privacy Commissioner. This office was amalgamated with, and served under, the newly created Office of the Australian Information Commissioner (‘OAIC’) in 2010. The Privacy Commissioner’s role is to regulate and monitor compliance under the Privacy Act.

B The Australian Law Reform Commission: Report 108

The Australian Law Reform Commission (‘ALRC’) examined the framework and effectiveness of the Privacy Act in a 28 month inquiry that led to the publishing, in 2008, of ‘Report 108: For Your Information: Australian Privacy Law & Practice’. The exploration of community attitudes towards privacy protection revealed concerns that rapid technological advances were eroding personal privacy.

The report emphasised the need for unified privacy principles that covered both public and private entities, the redefinition of terms, such as ‘sensitive information’, the accountability of entities engaging in cross-border data flow, and the introduction of heavy civil penalties for serious or repetitive privacy breaches. In all, the ALRC made 295 recommendations. An ‘emerging

---

384 Ibid.
385 Ibid.
386 Ibid.
388 Ibid vol 1, 105, 107.
389 Ibid vol 1, 110.
390 Ibid vol 1, 112.
391 Ibid vol 1, 126.
392 Ibid vol 1, 117.
393 Ibid vol 1, 103.
generation gap in basic attitudes to privacy and the impact of technology and social media was recognised.

Younger people, especially those born between 1980-1994 (‘Generation Y’) appeared willing to make available personal information in exchange for the convenience and range of internet services. Social networking, which involves public posting of thoughts, data, photographs and other personal information, was rapidly becoming the preferred method of communication between younger people. This group was also less likely to fully understand how the posting of personal information might adversely affect them.

Attitudes varied about the need for formal consent prior to online posting of personal information, including photographs, by a third party. The majority of respondents, however, reported that such information had, in fact, been posted without their knowledge or consent.

Fewer 18-24 year olds (50%) than the general adult population (69%) were aware of the existence of Commonwealth privacy laws. When awareness existed, respondents were often confused by the complexity and application of overlapping state and federal privacy laws. Which law covered federal or state government agencies and which private organisations? Differing privacy principles applicable to public agencies and private organisations (the Information Privacy Principles (‘IPPs’) and the National Privacy Principles (‘NPPs’)) only compounded this problem. Healthcare providers, key participants in collecting and managing private information, found the federal and state regulations difficult to navigate.

C The Privacy Amendment (Enhancing Privacy Protection) Act 2012

---

394 Ibid vol 1, 108.
395 Ibid vol 3, 2222.
396 Ibid vol 3, 2226.
397 Ibid vol 3, 2229.
398 Ibid vol 3, 2241.
400 Ibid vol 3, 2234.
401 Ibid vol 3, 2237.
402 Ibid vol 3, 2226.
403 Ibid vol 1, 109, 122.
404 Ibid vol 1, 109.
405 Ibid vol 1, 122.
The 2014 amendments to the Privacy Act incorporated many of the ALRC proposals. A new, unified set of privacy principles, the APPs, applied equally to Commonwealth public agencies and private organisations, replacing the IPPs and NPPs. Terms were updated or made consistent with other legislation; a ‘record’ now includes ‘electronic or other formats’ and new terms, such as ‘entity’ and ‘APP entity’ were introduced to aid the interpretation of new APPs.

Use of the term ‘sensitive information’ was expanded so that government agencies would have to distinguish it from ‘personal information’ a requirement that had not been present in the IPPs. Both federal government and private entities must employ additional precautions and security when collecting or handling ‘sensitive information’.

Previously biometric information, such as face or gait, could be ‘used without an individual’s knowledge or consent’; photographs ‘could be described as one of the lower levels of biometric recognition’. Biometric information was included in the expanded definition of sensitive information.

The privacy of ‘health information’ was especially important to respondents. ‘Health information’ was expanded to include the ‘physical, mental or psychological’ health or disability of an individual.

The Amendment Act made provisions for ‘permitted’ exceptions to accommodate circumstances where public interests outweigh personal privacy protection. Section 16A introduced seven ‘permitted general situations’ where APP entities may collect, use or disclose personal information without violating the Privacy Act. This can be seen for example, in s 16A, item 3(a), which states personal information may be

---

406 Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth).
408 Ibid vol 1, 112-3.
409 Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) sch 1 item 21.
410 Ibid sch 1 item 6.
413 Privacy Act 1988 (Cth) s 6(1) ‘sensitive information’; Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) sch 1 item 42.
414 Australian Law Reform Commission, above n 148, vol 1, 112.
415 Australian Law Reform Commission, above n 148, vol 1, 71.
collected, used or disclosed with the absence of consent, if the entity ‘reasonably believes’ the information would assist in locating the (reported) missing person. The test of ‘reasonableness’ is used here, as it is, liberally, through the Privacy Act and the APPs to indicate an objective assessment.

Section 16B allows for five ‘permitted health situations’ where consent is not required before an organisation collects, uses or discloses health information. A common example involves disclosure of a patient’s health information by a practitioner to another person who is responsible for the patient’s care.

The accountability approach contained within section 16C, for example, holds accountable a disclosing APP entity, in certain cases, for breaches that involve an ‘overseas [third party] recipient’. This includes situations where the overseas recipient is not subject to the APPs but engages in conduct that would breach the APPs if the scheme had applied.

Civil penalty provisions were added for serious or repeated inferences with privacy, as recommended by the ALRC. The Commissioner was empowered to apply to the court for an order against an entity that has allegedly contravened the Privacy Act. The maximum penalty a court can order against an individual is $360,000 and $1.8 million for entities.

---

416 See, eg, ‘reasonably necessary’, ‘reasonable steps’, ‘reasonably believes’.
417 Australian Government, above n 144, 53.
418 Privacy Act 1988 (Cth) s 16B(5)(d)(i).
419 Ibid s 16C(1)–(2).
420 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 226; The penalty is paid to the Commonwealth; Privacy Act 1988 (Cth) s 13G.
421 Federal Court or Federal Circuit Court.
422 Privacy Act 1988 (Cth) s 80W(1).
423 The value of one (1) penalty unit as at November 2016 is $180; Crimes Act 1914 (Cth) s 4AA. The Privacy Act 1988 (Cth) s 13G imposes a penalty of 2,000 penalty units for individuals who commit serious or repeated interferences with privacy, and s 80W(5) allows the court to make orders against contravening entities for a maximum of 5 times that of an individual.
1    *Australian Privacy Principles (APPs)*

The 13 Australian Privacy Principles are contained within Schedule 1 of the Privacy Act.\textsuperscript{424} They are further divided into Parts 1 through 5, each addressing separate aspects of privacy.

*Part 1: Management of Personal Information*
- APP 1 - open and transparent management of personal information
- APP 2 - anonymity and pseudonymity

*Part 2: Collection of Personal Information*
- APP 3 - collection of solicited personal information
- APP 4 - dealing with unsolicited personal information
- APP 5 - notification of the collection of personal information

*Part 3: Use and Disclosure of Personal Information*
- APP 6 - use or disclosure of personal information
- APP 7 - direct marketing
- APP 8 - cross-border disclosure of personal information
- APP 9 - adoption, use or disclosure of government related identifiers

*Part 4: Integrity, Quality & Security of Personal Information*
- APP 10 - quality of personal information
- APP 11 - security of personal information

*Part 5: Access to & Correction of Personal Information*
- APP 12 - access to personal information
- APP 13 - correction of personal information

Not confined solely to health information, the Privacy Act applies to all aspects of personal information privacy. Given the complexity and wide-ranging coverage of the Privacy Act, the Privacy Amendment Bill’s Explanatory Memorandum expressed the value in, and need for the OAIC to publish appropriately tailored APP guidelines.\textsuperscript{425} Where available OAIC draft guidelines\textsuperscript{426} have been used to discuss

\textsuperscript{424} Privacy Act 1988 (Cth) sch 1.
\textsuperscript{425} Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 53–55.
the APPs in reference to clinical images. This paper examines APP 3 and 5, dealing with collection, APP 6 and 8 restricting use and disclosure, and APP 11 addressing security, as they have greater bearing on, and pose increased compliancy challenges to, the practice of clinical photography.

Collection of Personal Information

The collection criteria for sensitive information, which includes health information, are more rigorous under APP 3.3, than for personal information. Collection of the information by governmental agencies must be for either a need that is ‘reasonably necessary’ or ‘directly related’ to the entity’s business activities or functions. Either criterion, ‘reasonably necessary’ or directly related’, must be accompanied by the individual’s consent. ‘[R]easonably necessary’ means a legitimate, objective need to justify an interference of privacy when collecting, using or disclosing personal information.

Organisations face tighter restrictions than governmental agencies. Organisations are authorised to collect sensitive information only if it is ‘reasonably necessary’ for the entity’s functions or activities. Obtaining the individual’s consent, however, is still required. Unlike agencies, organisations may not collect information unless it is reasonably necessary.

The OAIC’s draft business resource provides examples of collection such as storing patients’ ‘reasonably identifiable’ photographs, video or audio recordings, identifiable emails containing personal information and collecting and labelling

\[\text{\footnotesize \cite{426}}\]

Public consultation has been completed, and the new draft health privacy guidelines are currently being finalised. These guidelines are for guidance only and are not legislative instruments. For more information please see: Office of the Australian Information Commissioner, Australian Government, Advisory Guidelines <https://www.oaic.gov.au/agencies-and-organisations/advisory-guidelines/>.

\[\text{\footnotesize \cite{427}}\]

\textit{Privacy Act 1988 (Cth) s 6(1) ‘sensitive information’}.

\[\text{\footnotesize \cite{428}}\]

\textit{Ibid} sch 1 pt 2 sub–cl 3.1–3.2.

\[\text{\footnotesize \cite{429}}\]

‘Where collection, use or disclosure is reasonably necessary is to be assessed from the perspective of a reasonable person; Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 53.

\[\text{\footnotesize \cite{430}}\]

\textit{Privacy Act 1988 (Cth) sch 1 pt 2 sub–cl 3.3(a)(i).}

\[\text{\footnotesize \cite{431}}\]

Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 46, 53.

\[\text{\footnotesize \cite{432}}\]

\textit{Privacy Act 1988 (Cth) sch 1 pt 2 sub–cl 3.3(a)(ii).}

\[\text{\footnotesize \cite{433}}\]


\[\text{\footnotesize \cite{434}}\]

Australian Government, above n 142, 53.
patients’ biological samples. According to the OAIC guidelines storing clinical photographs in a patient’s record is ‘collection’. Practitioners may be in breach of APP 3.3(a)(ii) if patient consent is not obtained prior to taking and storing an identifiable photograph of a patient.

The Privacy Act does not apply if the patient’s image is not identifiable as it falls outside the definition of personal information. The consent requirement under the MBA Code is still applicable. Practitioners may rely on implied consent, though that should be documented. As previously discussed, implied consent may still raise ethical issues. The extent of implied consent, even when documented, may not be fully understood by the patient and leave the practitioner open to legal challenge.

APP 3.6 states that personal information should be collected directly from the person, though a measure of reasonableness is contained within this directive.

Second hand collection would not be a breach if it were ‘unreasonable’ to collect the information directly. The OAIC guidelines specifically make reference to the impracticality and unreasonableness of collecting personal information directly from the patient in circumstances of multi-disciplined care.

Patients are entitled to know, however, who has collected their information. Referring doctors should make patients aware of the team to whom they have been referred. If this is not directly achievable, the information recipient should notify the subject of the information collected.

An example illustrates this principle. A GP photographs a patient’s rash and emails the image to a dermatologist together with that patient’s details. The dermatologist assists the GP with diagnosis and stores the patient’s information even though the specialist may not interact directly with the patient. If the GP has not made the

---

435 Office of the Australian Information Commissioner, above n 433.
436 Privacy Act 1988 (Cth) s 6FA(b) defines ‘health information’ as ‘other personal information collected to provide, or in providing, a health service’; Mahar et al, above n 17, 48; Kirk et al, above n 23, 41; Hood, Hope and Dove, above n 23, 1009.
437 Privacy Act 1988 (Cth) s 6(1) definition of ‘consent’ includes express and implied.
439 Ibid sch 1 pt 2–cl 3.6(b).
440 Office of the Australian Information Commissioner, above n 433.
441 Reasonable efforts should be made to notify of the collection of personal information; Privacy Act 1988 (Cth) sch 1 pt 2–cl 5.1–5.2.
patient aware that the dermatologist has received, and therefore, collected their personal information, APP 5.1 obliges the dermatologist to take ‘steps as are reasonable in the circumstances’\(^{442}\) to notify the patient, about the collection of personal information, if not immediately, as soon as practicable.\(^{443}\) In contrast, if the dermatologist received a clinical image, and then deleted it after suggesting a diagnosis to the GP then, according to OAIC guidelines, no collection has occurred; notification principle (APP 5) would not apply.\(^{444}\)

**Use & Disclosure of Personal Information**

Once APP entities have collected personal information, APP 6 prescribes how they can use, and when they can disclose, personal information. Neither ‘use’ nor ‘disclosure’ are terms defined within the Privacy Act. This is left to the OAIC guidelines which states:

> ‘Generally, a use of health information occurs where you handle or undertake an activity with the information that you hold. A disclosure occurs where you make health information accessible to others outside your organisation and the subsequent handling of that information is released from your effective control.’\(^{445}\)

Examples of *use* include ‘accessing and reading a patient’s health information’ or ‘making a treatment decision based on a patient’s health information’, while *disclosure* examples cited are ‘sharing health information with another health service provider or individual’ or ‘providing a patient’s health information during a conversation with a person outside your organisation’.\(^{446}\)

The use and disclosure principle distinguishes between *primary* and *secondary* purposes, as an entity must not use or disclose personal information for a purpose other than that which it was collected for, without the individual’s consent.\(^{447}\) This clause is then qualified by an exception. If consent is not obtained, an entity may still use or disclose personal information, provided that it would be ‘reasonably expected’\(^{448}\). For *sensitive* information, such as health information, the secondary

---

\(^{442}\) Australian Government, above n 144, 53, 54.  
\(^{443}\) Privacy Act 1988 (Cth) sch 1 pt 2 sub–cls 5.1–5.2.  
\(^{444}\) Office of the Australian Information Commissioner, above n 433.  
\(^{445}\) Office of the Australian Information Commissioner, above n 243.  
\(^{446}\) Office of the Australian Information Commissioner, above n 243.  
\(^{447}\) Privacy Act 1988 (Cth) sch 1 pt 3 sub–cl 6.1.  
\(^{448}\) Australian Government, above n 144, 53.
purpose for using or disclosing the information must be *directly related* to the
primary purpose.\textsuperscript{449}

Clinical photographs are usually taken for a direct health benefit to the patient;
inclusion in the medical record or to facilitate diagnosis and/or treatment. That health
benefit would be the ‘primary purpose’ of collection. Use or disclosure for other
reasons would be considered a secondary purpose. For example, a photograph of a
patient used solely for staff to recognise the patient at reception or in the waiting
room, for security or convenience, would be a secondary purpose and require
consent. An identifiable image could not be used for publication without the patient’s
consent, because individuals would not reasonably expect that their clinical
photographs would be published. This is sensitive information and publishing has no
direct relationship to treatment; it would, therefore, be considered secondary to the
primary purpose of photographic documentation. Using and disclosing a patient’s
sensitive information for an indirectly related, secondary purpose is permitted only
where the patient grants consent.\textsuperscript{450}

The OAIC guidelines use the following example to illustrate when a patient would
reasonably expect disclosure:

> ‘When a general practitioner (GP) refers a patient to a specialist, most patients would
> reasonably expect that the specialist would disclose relevant information about the patient
> back to the GP.’\textsuperscript{451}

The APPs are not designed to obstruct or constrain genuine information flow needed
to facilitate proper provision of health care services. Sharing patients’ health
information among members of a treating team is often needed in multidisciplinary
care and consent in every case is not always reasonable or practical.\textsuperscript{452} APP 6
inclusion of a patient’s reasonable expectations as to how his or her information will
be disclosed is drafted to accommodate the ‘reasonable’ flow of important health
information, to necessitate appropriate care.

\textsuperscript{449} *Privacy Act 1988* (Cth) sch 1 pt 3 sub–cl 6.2(a)(i).
\textsuperscript{450} Ibid sch 1 pt 3 sub–cl 6.1(a).
\textsuperscript{451} Office of the Australian Information Commissioner, above n 243.
\textsuperscript{452} Ibid.
Doctors should proceed with caution before sharing patient information; not all disclosures to colleagues are appropriate, and ‘reasonably expected’ by patients. While *KJ v Wentworth Area Health Service* was based on state legislation this case emphasises the importance of clear doctor-patient communication. KJ’s sensitive information was shared between a team of healthcare providers responsible for her care. However, KJ alleged disclosure of her sensitive ‘psychological information’ was disclosed to practitioners who were not a part of the hospital’s healthcare team, without her knowledge or consent. This was held to be a breach of state privacy legislation, as it ‘constituted disclosure in the context of a large public sector agency’.

Although this case did not contravene the Privacy Act and did not involve clinical photographs, the disclosure of sensitive information is analogous to the use and disclosure of clinic images. The AMA recommends that practitioners take a few minutes to establish that the patient fully understands the reasons for taking the photographs, what they may be used for and to whom they may be disclosed. These simple steps may help mitigate the risk of potential litigation.

There are other exceptions to use and disclosure; for example, mandatory reporting (e.g. alleged child abuse), serious threat of harm and court ordered disclosures, though these types of disclosure are unlikely to occur frequently. Any disclosure required under federal, state or territory law is permissible under APP 6.2(b). Should an entity ‘reasonably’ believe disclosure is ‘necessary’ for any lawful enforcement related activities (e.g. photographic identification for intelligence gathering or investigation and prosecution of a criminal offence), the disclosing entity will not be in breach for unauthorised disclosure. Included in the Amendment Privacy Act were new exceptions under s 16A authorising disclosure in the case of ‘permitted general situations’. Disclosing a patient’s image for

---

454 Davis, above n 73, 120.
455 Privacy Act 1988 (Cth) sch 1 pt 3 sub–cl 6.2.
456 Australian Medical Association, above n 79.
457 Stevenson, Finnane and Soyer, above n 4, 198-9; Taylor et al, above n 70, 39.
458 See Privacy Act 1988 (Cth) s 16A, sch 1 pt 3 sub–cls 6.2(b)-(e).
459 All Australian jurisdictions are included; Office of the Australian Information Commissioner, above n 243.
460 For the Act’s definition of ‘enforcement body’ and ‘enforcement related activities’ see: Privacy Act 1988 (Cth) s 6(1).
461 Privacy Act 1988 (Cth) sch 1 pt 3 sub–cl 6.2(e).
photographic identification to assist locating a missing patient is one example where s 16A would apply.\textsuperscript{462}

APP 8.1 addresses cross border disclosure of personal information and where applicable, works in tandem with section 16C’s ‘accountability approach’. APP 8.1 states that prior to engaging in a cross border disclosure, the disclosing entity ‘\emph{must take such steps that are reasonable in the circumstances}’ to ensure the overseas recipient remains APP compliant. If reasonable steps are not taken, a disclosing entity may be held accountable if the overseas recipient breaches the APPs.\textsuperscript{463} This is in spite of the overseas recipient not being bound by the Australian Privacy Act and its APPs.\textsuperscript{464}

The accountability approach will not apply in certain circumstances. APP 8.2 outlines the exceptions when APP 8.1 will not apply to cross border disclosures. APP 8.2 states that provided the disclosing entity ‘reasonably believes’ that the overseas recipient is subject to similar enforceable privacy constraints, the entity will not be held accountable in the event of an overseas third party breach.\textsuperscript{465} Additionally, overseas disclosure for a ‘permitted general situation’\textsuperscript{466} falls within the exceptions, as does disclosure authorised by Australian law. APP 8.1 will also not apply where an entity is an ‘agency’ and disclosure of personal information occurs under an international agreement (regarding ‘information sharing’). Additionally, an agency that ‘reasonably believes’ that disclosure will aid enforcement related activities, will not be held accountable for a breach, provided the overseas enforcement agency powers parallel those in Australia.

To balance information flow and personal privacy,\textsuperscript{467} APP 8.2 was drafted to include a ‘consent’ clause. Individuals can grant consent for an APP entity to disclose their personal information to an overseas recipient, relieving the entity from

\textsuperscript{462} See \textit{Privacy Act 1988} (Cth) s 16A(1) item 3.
\textsuperscript{463} \textit{Privacy Act 1988} (Cth) s 16C (1)-(2), sch 1 pt 3 sub–cls 8.1–8.2.
\textsuperscript{464} Ibid s 16C (1)-(2), sch 1 pt 3 sub–cls 8.1–8.2.
\textsuperscript{465} Ibid sch 1 pt 3 sub–cl 8.2(a).
\textsuperscript{466} Ibid s 16A(1) item 1–3, 6–7.
\textsuperscript{467} Ibid s 2A.
accountability, should a breach occur. This is, however, conditional upon the entity expressly informing individuals of the effect of their consent, before they grant it.\(^{468}\)

The OAIC health guidelines state that when an entity gives others (outside of the entity) access to an individual’s personal information and no longer retains full control over how that information is handled, disclosure has occurred.\(^{469}\) Practitioners utilising cloud storage to back up or store clinical images, may be, (albeit inadvertently), disclosing sensitive information. Those, whose cloud providers are located outside Australia, would then be engaging in cross border disclosure. Further complicating the situation is that, the disclosing practitioner has not taken ‘reasonable steps’\(^{470}\) to ensure the overseas recipient will remain APP compliant, as is proscribed under APP 8.1.\(^{471}\) Assuming no exception applies under APP 8.2, and the overseas entity is not legally subject to Australian law, the practitioner would likely be held accountable for any third party breach by the overseas entity.\(^{472}\)

**Security of Personal Information**

Entities are, under APP 11, obligated to take ‘reasonable steps’\(^{473}\) to protect any personal information they hold, from misuse, interference or loss, unauthorised access, modification or disclosure.\(^{474}\)

The OAIC has not publicised its intention to develop specific security guidelines as part of their privacy guidance suite for health service providers. The OAIC has however, published a general guide: the ‘Guide to securing personal information: Reasonable steps to protect personal information’.\(^{475}\) It instructs entities to assess their risk exposure by considering factors such as network security, the use of encryption, email security affecting data transmission, password protection, as well

---

\(^{468}\) Ibid sch 1 pt 3 sub–cl 8.2(b).

\(^{469}\) Office of the Australian Information Commissioner, above n 243.

\(^{470}\) Australian Government, above n 144, 53, 54.

\(^{471}\) Privacy Act 1988 (Cth) s 16C (1) – (2), sch 1 pt 3 sub–cl 8.1.

\(^{472}\) Privacy Act 1988 (Cth) s 16C (1) – (2), sch 1 pt 3 sub–cl 8.1–8.2.

\(^{473}\) Australian Government, above n 144, 53, 54.

\(^{474}\) Privacy Act 1988 (Cth) sch 1 pt 4 cl 11.1.

as storage and back up. The guide then recommends that entities develop and institute policies and practices to manage these risks.

Practitioners using digital clinical photography may be affected by the above-mentioned factors, presenting security risks surrounding the protection of personal information. Emailing unencrypted clinical photographs from a smartphone poses security risks, as does storing unencrypted images on portable storage devices (e.g. USB thumb drives and SD cards). Physical loss or theft is yet another risk of any mobile device and invites unauthorised access if password protection is absent. Using cloud providers (often located overseas) for storage and back up, not only creates possible trans-border disclosure compliance issues, but has the potential to amplify the security risks confronting a practitioner through multiple device synchronisation.

Consider the issues presented where practitioners co-opt personal smartphones for use in practice, a common practice amongst doctors. They may back up their personal smartphones to their cloud provider, where a doctor’s clinical photographs can, through auto-synchronisation, appear on as many devices as are using the account; for example, where clinical photos are synced to the practitioner’s wife’s smartphone, as the cloud account is shared between them. In such an event, disclosure breaches will have been triggering. Added to this is that synchronisation can cause multiple copies of clinical images to appear on numerous synced devices, rapidly increasing the risk of one or more security breaches occurring.

2 Breach of the Privacy Act

The Australian Privacy Principles, designed to protect personal information, provides the core structure around which the Privacy Act is built. These underlining principles are to be upheld unless an exception applies. Section 6A states that an act or practice that is ‘contrary to, or inconsistent with’ one or more of the APPs, is a breach

---

476 Ibid.
477 Stevenson, Finnane and Soyer, above n 4, 198.
478 Privacy Act 1988 (Cth) s 6A(1).
unless the Privacy Act excludes it. Consequently, a breach of an APP is deemed an ‘interference with the privacy of an individual’.  

The OAIC will not always apply a pecuniary penalty in all cases of breach; for example, in cases of minor or inadvertent contraventions where the entity has cooperated with OAIC’s investigation (if applicable) and has taken steps to prevent a repeat occurrence. The Privacy Act empowers the Privacy Commissioner to conduct discretionary assessments, to investigate matters where complaints have been made, or to commence a ‘Commissioner Initiated Investigation’ where conduct indicates possible APP non-compliance. The Commissioner may then make an enforceable determination outlining the requirements to rectify the breach and preventative action needed to avoid future breaches. The determination may include a compensatory payment for loss or damage, which is not confined to financial loss and can be awarded for emotion distress. Alternatively, the Commissioner may prefer to seek a court order.

Serious or repeated privacy breaches are addressed by s 13G, a ‘civil penalty provision’, which can attract a civil penalty of up to $360,000 for individuals and $1.8 million for entities. Although dealt with in a single section, serious and repeated interferences are separate concepts, and the civil penalty can only be made by court order, following the Commissioner application. The affected party may also seek a compensatory order for loss or damage, both pecuniary, and non-

---

Ibid ss 6A(2)–(5), 13B–D.
Ibid (Cth) s 13(1)(a).
Privacy Act 1988 (Cth) s 33C.
Ibid s 40(1).
Ibid s 40(2).
Ibid s 55A.
Ibid s 52(1)(b)(ia).
Ibid s 52(1)(b)(iii).
Ibid s 52(1AB); Explanatory Memorandum, Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Cth) 245.
Privacy Act 1988 (Cth) s 80W.
See Privacy Act 1988 (Cth) s 80U regarding the Act’s sections or subsections that are penalty provisions.
Above n 423.
Privacy Act 1988 (Cth) s 13G.
The Office of the Information Commissioner, Australian Government, above n 481.
See Privacy Act 1988 (Cth) s 80W(1) stipulates an application to the court must be within 6 years of the alleged contravention.
pecuniary, provided loss or damage can be established.\(^{495}\) The court retains discretionary power to determine the value of a civil penalty,\(^{496}\) if satisfied the entity has contravened the Privacy Act.\(^{497}\) An individual may be ordered to pay a penalty limited by the maximum value prescribed in the contravened section,\(^{498}\) while entities could be made to pay up to 5 times the maximum prescribed for individuals.\(^{499}\)

The Privacy Act does not define the terms ‘serious’ or ‘repeated’, but should be given their ordinary meaning,\(^{500}\) and determined objectively from a reasonable person’s view.\(^{501}\) When assessing if a contravention is serious, the Commissioner will give heed to the extent and impact of the breach, the type of information that was affected (e.g. sensitive information), possible or manifested consequences for the affected person(s), and the circumstances that led to the breach (e.g. inadvertent mistake or carelessness).\(^{502}\)

Repeat breaches must arise from separate instances of contravening conduct; multiple breaches of different provisions, arising from ‘one act or practice’ will not be seen as a repeat contravention.\(^{503}\) In cases of repeat contraventions, the Commissioner will be more likely to seek a penalty order where the offending party has disregarded privacy obligations and failed to prevent further breaches.\(^{504}\)

Although the Commissioner can seek determinations concurrently where two or more penalty provisions are breached in a single incident, the court cannot make multiple orders against the contravener. Instead the court may only penalise the individual or entity for contravening one penalty provision, arising from a single incident.\(^{505}\)

\(^{495}\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 194-5.
\(^{496}\) After considering the context of the breach, the circumstances, the loss or damage sustained and previous conduct; Privacy Act 1988 (Cth) s 80W(6)(a)–(b).
\(^{497}\) The penalty is paid to the Commonwealth; Privacy Act 1988 (Cth) s 80W(1).
\(^{498}\) To the maximum value of $360,000; Privacy Act 1988 (Cth) ss 13G, 80W(3).
\(^{499}\) To the maximum value of $1,800,000; Privacy Act 1988 (Cth) ss 13G, 80W(5).
\(^{500}\) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 226.
\(^{501}\) Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Cth) s 26WB ‘sets out the circumstances in which a ‘serious data breach’ occurs.’ If enacted, the amendment will address how to assess if a breach is considered a ‘serious’ breach under s 13G of the Privacy Act.
\(^{502}\) If the Privacy Amendment (Notification of Serious Breaches) Bill is enacted, it will provide a definition for ‘serious breach’; Explanatory Memorandum, Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Cth) 10.
\(^{503}\) The Office of the Information Commissioner, above n 481.
\(^{504}\) Ibid.
\(^{505}\) Privacy Act 1988 (Cth) s 80Y.
In contrast, where an entity breaches the same provision numerous times, the court may make one single order, the total value not exceeding the sum of the maximum penalty that could be order if separate orders were issued.\textsuperscript{506} For instance, if an individual contravened s 13G on 3 separate occasions, the total sum contained in the court order cannot exceed 3 times the maximum penalty of s 13G. Any civil penalty is payable to the Commonwealth and is an enforceable debt,\textsuperscript{507} and affected individuals are not compensated by this order.\textsuperscript{508}

There are, to date, no privacy breaches under the reformed Privacy Act that involve clinical photographs. There has, however, been one OAIC determination made in June 2016. The practitioner made unauthorised disclosures via email, in breach of APP 6.1 and was made to pay the affected patient $10,000 in compensation.\textsuperscript{509} Then in late October 2016 the disquieting Australian Red Cross Blood Service database breach was announced. It involved 550,000 Australians who had registered to donate blood.\textsuperscript{510} This incident is believed to be Australia’s largest data breach incident to date.\textsuperscript{511} The company contracted to manage, support and maintain the Red Cross IT systems, through human error, made these files which contained completed donor application forms, publically available online.\textsuperscript{512} The security lapse extended over a seven week period before the error was discovered where personal details of donor applicants, such as names, birthdates and contact details contained within the application form were exposed. These forms also included donor answers to the highly sensitive yes/no question: ‘In the last 12 months, have you engaged in at-risk sexual behaviour?’\textsuperscript{513}

All donor applicant information was provided in connection with the intended donation of blood, and is thus health information under the Privacy Act.\textsuperscript{514} For this

\textsuperscript{506} The Office of the Information Commissioner, above n 481.
\textsuperscript{507} Privacy Act 1988 (Cth) s 80X; Note: Compensation orders under sections 25, 25A only apply to credit reporting.
\textsuperscript{508} Privacy Act 1988 (Cth) s 80W; The Office of the Information Commissioner, above n 481.
\textsuperscript{509} ‘IV’ and ‘IW’ [2016] AlCmr 41 (27 June 2016).
\textsuperscript{512} Australian Red Cross Blood Service, above n 510.
reason each individual’s entire information set is sensitive information.\(^{515}\) The OAIC has been notified and an investigation is forthcoming.\(^{516}\)

Other data breaches prompting OAIC to investigate have occurred over the past two years, however, none concerned health information. Retail online divisions of K-Mart, David Jones, and Aussie Travel Cover were hacked between December 2014 and October 2015. Personal information such as names, email and postal addresses, and financial information were accessed. The K-Mart and David Jones incidences are currently under investigation by the OAIC,\(^{517}\) though the Commissioner has finalised his investigation into the Aussie Travel Cover (‘ATC’) data breach. Despite the details of 137 records being stolen due to website vulnerabilities, neither a compensatory declaration was made, nor a pecuniary penalty order sought against ATC.\(^{518}\) The OAIC cited sufficient security changes made by ATC as the reason for this decision.\(^{519}\)

Initially it was thought that the ATC incident had compromised up to 750,000 individuals’ personal information. The company alerted ‘third party agents’ of the breach 5 days after the incident, but advised there was no need to alert insurance policy holders or customers.\(^{520}\) OAIC’s investigation revealed almost all the data was corrupted in the extraction process, with the hackers only retrieving 133 agencies and 4 policy holders’ data successfully; these affected entities and individuals were then informed. It appears that this notification came long after the incident.\(^{521}\) No doubt this news was met with great relief from ATC and the majority of its agents and customers. Given the gravity of the situation, however, and the

---

514. *Privacy Act 1988* (Cth) s 6FA(c) ‘Meaning of health information’ includes donation or intended donation of body substances.

515. Ibid ss 6(1), 6FA(c) Health information is sensitive information.


521. Ibid; Office of the Australian Information Commissioner, above n 518.
potential for identity theft, as a result of stolen identification information, were these customers not entitled to know that their information might have been compromised? Should customers not be given the opportunity to take counter measures if they feel it is necessary? Notification in this case would have been a false alarm for the majority in this instance, however, initially, it would appear ATC could not have known this. Certainly some would argue this incident was deserving of some form of pecuniary penalty.

The Australian Parliament is currently considering the ‘Mandatory Data Breach Notification Bill’ and if successful, the legislation will oblige the affected entity to report breaches to both the OAIC and any affected individuals. These measures, would in turn, remove from the entity the option of concealing the breach, ensuring affected individuals are able to make their own choice about how to respond. The Centre of Internet Safety report revealed that ‘85% of online Australians believe data breach notification should be mandatory for business’ however, this sentiment is not confined to the business arena. A 2012 patient survey showed that 75.3% of patients supported stronger enforcement of privacy laws, asserting such measures would encourage healthcare providers to familiarise themselves with their privacy obligations, thus lowering the chances of a breach.

The above-mentioned breaches have compromised personal information entrusted to entities, highlighting the importance of establishing and implementing sufficient security measures. Many practitioners are not taking adequate security precautions, and putting patients’ sensitive information at risk because they do not realise the potential consequences of their actions. What is the cause for this knowledge deficit and what role does the OAIC have in improving the situation? This raises many questions. Should the Privacy Commissioner take a harsher approach, by increasingly seeking civil penalty orders for breaches? Would this increase awareness of privacy obligations? How would this impact entities security

522 For example, putting stops on credit cards and changing credit card details.
524 New London Consulting, above n 45.
525 Privacy Act 1988 (Cth) sch 1 pt 4 sub-cl 11.1.
practices? Although there are several OAIC assessments, presently there are insufficient determinations by the Privacy Commissioner to examine the issue adequately.

We can, however, see the US outcomes of strict regulatory enforcement of (non-photographic) health information privacy breaches. US federal law, the ‘Health Information Technology for Economic and Clinical Health Act 2009’ (US) (‘HITECH Act’) provides for mandatory notification applicable to health data breaches. The HITECH Act supports and extends the ‘Health Insurance Portability and Accountability Act 1996’ (US) (‘HIPAA’), which lays out health information privacy, security and enforcement requirements. To this was added the HIPAA ‘Final Rule’ (also referred to as the ‘Omnibus Rule’) coming into force in September 2013. By introducing this amendment, parties associated with entities coming under the Acts, were caught by the privacy legislation net, further strengthening privacy protection of health information. Hefty regulatory fines are now strictly enforced by the privacy regulator – the Office for Civil Rights (‘OCR’) Department of Health and Human Services (‘HHS’). This came about following a period of public dissatisfaction over the leniency of pecuniary penalty implementation. In 2014 a HHS media release published detailed that New York and Presbyterian Hospital and Columbia University suffered a joint breach due to inadequate security systems. This caused the health information of 6,800 individuals to become publically available online. The hospital and university settled the HIPAA violations with the OCR for $4.8 million. Similarly, a network configuration error made by St Joseph Health saw the health organisation settle an unauthorised

526 Office of the Australian Information Commissioner, above n 34.
529 42 USC § 1320d.
531 Ibid.
532 Rinehart-Thompson, Hjort and Cassidy, above n 528, 1–3.
disclosure breach for $2.14 million.\(^{534}\) Again, another HIPAA breach that was avoidable had proper security precautions been instituted. Stimulating media coverage, these penalties provide the impetus for healthcare providers to understand their obligations to prevent incurring fines.

VI CONCLUSION

A The Problem Re-visited

It appears that technology and privacy, to some degree, share an inverse relationship; technological advancement frequently sees a further decline in privacy. As the literature suggests, using digital photography in a clinical setting offers many benefits to assist with, and improve patient care; it must, however, be used within the bounds of privacy laws and professionals codes so as not to jeopardise patient privacy. A proper understanding of the perils posed by digital photography is necessary for practitioners to safeguard against unnecessary and avoidable risks. Educating medical practitioners of their legal and professional privacy obligations is one way of addressing the disparity between current digital photography practices and these privacy obligations.

This paper explored the use of digital photography within medicine, and the effects this technology has had on personal privacy, in light of the reformed Privacy Act. Despite photography being the focal point, it is illustrative of a larger problem – it is becoming increasingly easier to violate a patient’s privacy through the adoption and use of technology within healthcare. Consider the Australian Red Cross data breach incident of October 2016; what are the consequences of this privacy violation, not yet manifested? It is vital that those in whom sensitive information is entrusted sufficiently understand how to protect it. Preferring a proactive approach, to a reactive response (i.e. damage control) may avert potential harm that cannot be reversed.

B Increased Education - A Proactive Approach

As privacy is an area that touches all patients, it is proposed that compulsory education be introduced as a regulatory requirement. Collaboration between the OAIC, AHPRA or the Medical Board and the RACGP and medical indemnity insurers will allow the development of a comprehensive tailored training module, teaching practitioners how to maintain patient privacy while maximising utility offered by technology, facilitating optimum patient care. The proposed educational
module need not be confined to digital photography for clinical practice, but could extend to other everyday technological clinical tools (e.g. EMRs, practitioner-patient email communications). Emphasis must be on the legal obligations introduced by the Privacy Act, and applicable professional obligations. Digitised information facilitates quick and easy dissemination that may breach legal and professional obligations if not dealt with correctly. Practitioners cannot take steps to mitigate risks they are unaware of, though lack of awareness does not alleviate responsibility. Doctors should be provided with information that clearly illustrates how current practices may not only increase the risk of breach, but may already be contrary to federal law. Awareness of legal penalties including litigation, in addition to professional sanctions, for a breach, should encourage safer practices.

The numerous issues surrounding digital photography, as explored in this paper, bear directly upon practitioners’ practices of collection, use and disclosure of patients’ photographs. Digital media education must comprehensively examine these privacy requirements and doctors must be informed that a divergence from these obligations is only permissible when covered by a specific legal and/or professional exception. The other key concept that sets aside applicable privacy obligations is valid patient consent.

Training must emphasise that consent continues to apply to clinical photography, and should be obtained, as it would for any other treatment. The key elements of valid consent equally apply. Patients must not be cajoled into consenting; consent must be given freely. Doctors should fully explain to the patient why the photograph is necessary, outlining its associated benefits and risk (e.g. interference and unauthorised disclosure) prior to obtaining consent. If the photograph is needed for treatment purposes, the doctor should inform the patient of the possible disclosure to other members of the treating team. If a specialist consultation might be required, this must be disclosed to the patient. When photographing a patient, the frame should only include that which is necessary, in an attempt to preserve anonymity. Although verbal consent is sufficient for photographic documentation, (and should always be documented) practitioners should be encouraged to obtain written consent. Consent for educational or publishing purposes should always be in written form for medico-legal reasons.
Practical training must include security practices and procedures that if followed, will significantly mitigate the risk of using digital photography in a clinical environment. Common pitfalls need to be highlighted so practitioners are aware of these issues, such as cloud storage. Non-compulsory training often results in non-attendance, and therefore, may not be effective in significantly reducing the knowledge deficit as identified.

C Indoctrination of Hospital-based Junior Doctors

The lack of medical professionalism amongst the younger generation of doctors is of growing concern, due to the attitudes and behaviours demonstrated by this group of practitioners. Social media is part of daily life for many young adults and has permeated the professional workplace, not being confined to the personal sphere. Smartphone photography has been embraced across cultures and societies and rarely provokes much thought before a picture is taken. This unremarkable practice, appropriate in a personal context, has seeped through the porous divide separating professional from personal. Smartphone photography should not be transplanted into the practice of medicine until junior practitioners understand how to mitigate the accompanying risks.

All new medical graduates are required to participate in a 47 week FTE internship, which is largely hospital-based, before they can acquire general registration; this may provide the opportune educational structure for incorporation of a digital media module. Content should include doctors’ legal and professional privacy

535 Kornhaber, Betthavas and Baber, above n 6, 301.
537 Carruth and Ginsburg, above n 264, 83.
538 Sánchez Abril, Levin and Del Riego, above n 7, 64.
539 Internship is a period of mandatory supervised general clinical experience. It allows medical graduates to consolidate and apply clinical knowledge and skills while taking on increasing responsibility for the provision of safe, high quality patient care. Diagnostic skills, communication skills, management skills, including therapeutic and procedural skills, and professionalism are developed under appropriate supervision; Medical Board of Australia, Interns: Registration Standard – Granting General Registration as a Medical Practitioner to Australian and New Zealand Medical Graduates on Completion of Intern Training <http://www.medicalboard.gov.au/documents/default.aspx?record=WD12%2f9504%5b5v%5d&dbhid=AP&chksum=PvYzX0nEO%2bYT0wNVgblkA%3d%3d>.
540 Health Practitioner Regulation National Law (WA) Act 2010 (WA) s 52; Medical Board of Australia, above n 539.
541 A similar hospital based approach was suggested by Van der Rijt and Hoffman, above n 6, 212.
obligations as it applies to use of clinical photography and social media, with a specific component addressing safe practices and risk management. Cognisance of the consequences that can stem from inappropriate use of photography, including professional and legal sanctions, which can affect their career, may provide the impetus needed to alter this behaviour. Educating young doctors as they enter the profession may ingrain safe practices, which they may take with them to other specialty areas, including general practice.

D Continuing Professional Development Training

General practice is not a predominantly visually focused specialty, however the RACGP offers a ‘Certificate of Primary Care Dermatology’. Practitioners consulting in this specialised general practice area are likely to use clinical photography. A module on privacy compliance and clinical photography may be an appropriate in courses such as these.

Certain visually oriented medical specialties that commonly use clinical photography (e.g. dermatology, general and plastic surgery) belong to specialist colleges regulated by the MBA. These specialist colleges (e.g. Australasian College of Dermatologists, Royal Australasian College of Surgeons) may be well placed to require compulsory training in privacy and digital clinical imagery if they manage an accredited CPD program. As with any dynamic profession, regular training facilitates ongoing learning as developments progress.

Though not yet in place, the MBA is examining the model of ‘revalidation’. Its purpose would be to ‘maintain and enhance their [medical practitioners] professional skills and knowledge and to remain fit to practice medicine’. The revalidation components would compose of ‘strengthened CPD’ programs, and identifying and supporting poorly performing doctors, with a focus on keeping doctors’

542 Chretien et al. suggested a similar approach, though it was pos as a undergraduate medical degree module targeting aimed at medical students was suggested by Chretien et al, above n 273, 1313.
543 RACGP, above n 209.
544 Mahar et al, above n 17, 48.
546 Ibid.
knowledge up-to-date.\textsuperscript{547} If implemented, CPD training will aim to be ‘more effective, flexible and dynamic’.\textsuperscript{548} Revalidation may present another avenue in which a general privacy and technology CPD module could be incorporated. Once again, the MBA can regulate that visually oriented specialties complete an in depth course on privacy obligations and clinical photography where appropriate.

E \textit{Final Comments}

The amendments made to the Privacy Act have strengthened protections for personal information and prescribed stricter conditions that limit how APP entities handle the information they hold. These standards, when applied to clinical photography, create legal pitfalls easily missed by practitioners who may not be cognisant of the privacy obligations they incur by incorporating digital photography into their practice.

Complicating the situation further are inconsistencies between the Privacy Act, the National Law and the MBA Code. The Privacy Act determines the minimum standards of privacy protection, significant differences exist between the Privacy Act, the National Law and the Code that make the existing privacy framework difficult to navigate.

In the short term, GPs may benefit from clear and comprehensive guidelines issued by the OAIC which explain the privacy obligations of using clinical photography.\textsuperscript{549} The OAIC should ensure its information is distributed to all health practitioner regulatory bodies, such as AHPRA, the Medical Board and the specialty medical colleges like the RACGP. With time, there will develop a body of case law that reflects a deeper understanding of how the reformed Privacy Act affects healthcare practices. This will encourage further investigation into the effectiveness of OAIC related penalties to raise awareness or act as a deterrent.

\textsuperscript{547} Medical Board of Australia, \textit{Medical Board Consults on Revalidation in Australia} (16 August 2016) \newline \textltt{<http://www.medicalboard.gov.au/News/2016-08-16-revalidation.aspx>}.

\textsuperscript{548} Medical Board of Australia, above n 545.

\textsuperscript{549} The OAIC’s current information on mobile phone photography lacks depth and does not warn practitioners of the extensive risk (e.g. security risks with cloud storage) that may be involve in this practice; Office of the Australian Information Commissioner, Australian Government, above n 206.
For this reason, privacy and technology education may assist practitioners in understanding their legal and professional obligations. The OAIC, AHPRA or the Medical Board of Australia should collaborate with the RACGP and the medical defence organisations to develop and offer an appropriate training module. Using the organisations that have frequent contact with GPs is the most direct way to help GPs understand and observe the new privacy laws and regulations. Like safe driving classes, dedicated clinical photography training may not only improve compliance but also reassure and encourage doctors to add this valuable tool to help promote their patients’ health.
VII ANNEXURES

Annexure A

*The Australian Health Practitioner Regulation Agency National Boards*

1. Aboriginal and Torres Strait Islander Health Practice Board
2. Chinese Medicine Board of Australia
3. Chiropractic Board of Australia
4. Dental Board of Australia
5. Medical Board of Australia
6. Medical Radiation Practice Board of Australia
7. Nursing and Midwifery Board of Australia
8. Occupational Therapy Board of Australia
9. Optometry Board of Australia
10. Osteopathy Board of Australia
11. Pharmacy Board of Australia
12. Physiotherapy Board of Australia
13. Podiatry Board of Australia
14. Psychology Board of Australia
Annexure B

State and Territory Medical Boards

1. The ACT Board of the Medical Board of Australia
2. The New South Wales Board of the Medical Board of Australia
3. The Northern Territory Board of the Medical Board of Australia
4. The Queensland Board of the Medical Board of Australia
5. The South Australian Board of the Medical Board of Australia
6. The Tasmanian Board of the Medical Board of Australia
7. The Victorian Board of the Medical Board of Australia
8. The Western Australian Board of the Medical Board of Australia
### Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accountability Approach</strong></td>
<td>APP Entity who makes a disclosure to an overseas recipient, will be held accountable for the recipient’s APP breach in some circumstances; <em>Privacy Act</em> section 16C, APP 8</td>
</tr>
<tr>
<td><strong>Agency</strong></td>
<td>Refer to section 6(1) of the <em>Privacy Act</em></td>
</tr>
<tr>
<td><strong>APP Entity</strong></td>
<td>An ‘agency’ or ‘organisation’ as defined in section 6(1) – ‘Entity’ of the <em>Privacy Act</em></td>
</tr>
<tr>
<td><strong>Australian Privacy Principles</strong></td>
<td>Schedule 1 of the <em>Privacy Act</em></td>
</tr>
<tr>
<td><strong>APP Breach</strong></td>
<td>Refer to section 6A of the <em>Privacy Act</em></td>
</tr>
<tr>
<td><strong>Civil Penalty Order</strong></td>
<td>Refer to section 80W(4) of the <em>Privacy Act</em></td>
</tr>
<tr>
<td><strong>Civil Penalty Provision</strong></td>
<td>Refer to section 80U of the <em>Privacy Act</em></td>
</tr>
<tr>
<td><strong>Clinical Photography</strong></td>
<td>A photograph taken for medical purposes (also referred to as digital photography or clinical image)</td>
</tr>
<tr>
<td><strong>Cloud Storage</strong></td>
<td>Data storage where the digital data is stored in logical pools, the physical storage is across multiple servers and locations, and the physical environment is typically owned and managed by a hosting company</td>
</tr>
<tr>
<td><strong>Code / MBA Code</strong></td>
<td>The Medical Board of Australia’s Professional Code of Conduct: Good Medical Practice</td>
</tr>
<tr>
<td><strong>Collects</strong></td>
<td>An entity collects personal information only if the entity records that information in a record; <em>Privacy Act</em> s 6(1)</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Consent</td>
<td>Permission given by someone to do something to his or her person. Consent can be either express or implied</td>
</tr>
<tr>
<td>De-identified information</td>
<td>Information is de-identified if it is ‘no longer about an identifiable individual or an individual that is reasonably identifiable’ as defined by section 6 of the Privacy Act</td>
</tr>
<tr>
<td>Dermatologist</td>
<td>A medical practitioner that specialises in skin</td>
</tr>
<tr>
<td>Entity</td>
<td>An agency, organisation or small business operator</td>
</tr>
<tr>
<td>Health Information</td>
<td>Any information or opinion about an individual’s health, including illness, disability or injury and health services sought or provided, whether presently or in the future. Health information also includes any personal information collected to provide, or while providing a health service; as defined by section 6FA of the Privacy Act</td>
</tr>
<tr>
<td>Health Service</td>
<td>Refer to section 6FB of the Privacy Act</td>
</tr>
<tr>
<td>Health Service Provider</td>
<td>A provider of health services, or holder of health information, even if providing health services is not the organisation’s primary function or activity</td>
</tr>
<tr>
<td>General Practitioner (GP)</td>
<td>A medical practitioner/doctor who specialises in general practice</td>
</tr>
<tr>
<td>Interference (of privacy)</td>
<td>Refer to section 13–13F of the Privacy Act</td>
</tr>
<tr>
<td>Lesion</td>
<td>An irregular region of external body tissue affected by disease</td>
</tr>
<tr>
<td>Permitted General Situation</td>
<td>Refer to section 16A of the Privacy Act</td>
</tr>
<tr>
<td>Permitted Health Situation</td>
<td>Refer to section 16B of the Privacy Act</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Personal information</strong></td>
<td>Information, whether fact or opinion, about a specific individual who is identified or reasonably identifiable; defined by s 6(1) of the Privacy Act</td>
</tr>
<tr>
<td><strong>Organisation</strong></td>
<td>An individual, body corporate, partnership, any other unincorporated association or a trust, that is not a small business operator, a registered political party, an agency, or a state / territory authority or a state/territory prescribed instrumentality; defined by section 6C of the Privacy Act</td>
</tr>
<tr>
<td><strong>Practitioner</strong></td>
<td>A licensed medical practitioner (a doctor)</td>
</tr>
<tr>
<td><strong>Primary Purpose</strong></td>
<td>The main reason behind the action for collection, use or disclosure</td>
</tr>
<tr>
<td><strong>Private Entity</strong></td>
<td>Any organisation not owned by the Australia Government</td>
</tr>
<tr>
<td><strong>Public Entity</strong></td>
<td>Any Australian Government Agency Australian</td>
</tr>
<tr>
<td><strong>Reasonableness</strong></td>
<td>The appropriateness of decision-making that reflects an objective standard having regard to the circumstances and context (see LexisNexis Concise Australian Legal Dictionary, 4th ed)</td>
</tr>
<tr>
<td><strong>Record</strong></td>
<td>A document, electronic device or other device as defined in s 6(1) of the Privacy Act</td>
</tr>
<tr>
<td><strong>Registrar</strong></td>
<td>A registered medical practitioner who has is undertaking specialty accredited training (e.g. a doctor who is training in dermatology)</td>
</tr>
<tr>
<td><strong>Responsible Person</strong></td>
<td>Refer to section 6AA of the Privacy Act</td>
</tr>
<tr>
<td><strong>Secondary Purpose</strong></td>
<td>Any purpose that is not the primary purpose</td>
</tr>
<tr>
<td><strong>Store and forward</strong></td>
<td>A process where the original party records information, for example, a photograph, then electronically transmits a copy to another party</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Sensitive Information</strong></td>
<td>Information or opinion about an individual’s health or genetic information, biometric information used for identification purposes, biometric templates, sexual orientation or practices, race, ethnicity, political opinions, political associations, religious or philosophical beliefs, membership of a professional or trade union/association</td>
</tr>
<tr>
<td><strong>Small Business Operator</strong></td>
<td>Refer to section 6D of the <em>Privacy Act</em></td>
</tr>
<tr>
<td>ACRONYMS</td>
<td>FULL NAME</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>ACT</td>
<td>Australian Capital Territory</td>
</tr>
<tr>
<td>ACGP</td>
<td>Australian College of General Practitioners</td>
</tr>
<tr>
<td>AHPRA</td>
<td>Australian Health Practitioner Regulation Agency</td>
</tr>
<tr>
<td>ALRC</td>
<td>Australian Law Reform Commission</td>
</tr>
<tr>
<td>AMA</td>
<td>Australian Medical Association</td>
</tr>
<tr>
<td>APPs</td>
<td>Australian Privacy Principles</td>
</tr>
<tr>
<td>ATC</td>
<td>Aussie Travel Cover</td>
</tr>
<tr>
<td>AUS</td>
<td>Australia</td>
</tr>
<tr>
<td>CPD</td>
<td>Continuing Professional Development</td>
</tr>
<tr>
<td>CPR</td>
<td>Cardiopulmonary resuscitation</td>
</tr>
<tr>
<td>ED</td>
<td>Emergency Department</td>
</tr>
<tr>
<td>EMR</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>GMC</td>
<td>General Medical Council (UK)</td>
</tr>
<tr>
<td>GP</td>
<td>General Practitioner</td>
</tr>
<tr>
<td>HHS</td>
<td>Health and Human Services, US Department of</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act 1996</td>
</tr>
<tr>
<td>HITECH</td>
<td>Health Information Technology and Economic Clinical Health Act</td>
</tr>
<tr>
<td>IPPs</td>
<td>Information Privacy Principles</td>
</tr>
<tr>
<td>MBA</td>
<td>Medical Board of Australia</td>
</tr>
<tr>
<td>MIIAA</td>
<td>Medical Indemnity Industry Association of Australia</td>
</tr>
<tr>
<td>NPPs</td>
<td>National Privacy Principles</td>
</tr>
<tr>
<td>NRAS</td>
<td>National Registration and Accreditation Scheme</td>
</tr>
<tr>
<td>NSW</td>
<td>New South Wales</td>
</tr>
<tr>
<td>NT</td>
<td>Northern Territory</td>
</tr>
<tr>
<td>OAIC</td>
<td>Office of the Australian Information Commissioner</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Name</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>OCR</td>
<td>Office of Civil Rights (US)</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Cooperation and Development</td>
</tr>
<tr>
<td>QLD</td>
<td>Queensland</td>
</tr>
<tr>
<td>RACD</td>
<td>Royal Australian College of Dermatologists</td>
</tr>
<tr>
<td>RACGP</td>
<td>Royal Australian College of General Practitioners</td>
</tr>
<tr>
<td>RACS</td>
<td>Royal Australian College of Surgery</td>
</tr>
<tr>
<td>RCGP</td>
<td>Royal College of General Practitioners (UK)</td>
</tr>
<tr>
<td>SA</td>
<td>South Australia</td>
</tr>
<tr>
<td>TAS</td>
<td>Tasmania</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UCSF-MC</td>
<td>University of California, San Francisco Medical Centre</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>VIC</td>
<td>Victoria</td>
</tr>
<tr>
<td>VR</td>
<td>Vocational Registration</td>
</tr>
<tr>
<td>WA</td>
<td>Western Australia</td>
</tr>
<tr>
<td>WMA</td>
<td>World Medical Association</td>
</tr>
</tbody>
</table>
X  BIBLIOGRAPHY

A  Articles/Books/Reports

Allan, Sonia and Meredith Blake, The Patient and the Practitioner: Health Law and Ethics in Australia (LexisNexis Butterworths Australia, 2014)


Amaboo, Dhai and Jason Payne-James, ‘Problems of Capacity, Consent and Confidentiality’ 2013 27 Best Practice & Research Clinical Obstetrics and Gynaecology 59

Baldwin, Yvonne, ‘Peril of the Pic’ 2010 4 First Defence MDA National 4

Beauchamp, Tom and James Childress, Principles of Biomedical Ethics (Oxford University Press, 6th ed 2009)

Berlant, Jeffrey, ‘Profession and monopoly: A study of medicine in the United States and Great Britain’ 1976 20(3) Medical History 342


Berle, Ian, ‘Clinical Photography and Patients’ Rights: The Need for Orthopraxy’ 2008 34 Journal of Medical Ethics 89


Burns, Kara, ‘Smartphones in Medicine Need to be Smarter’ 2013 3(3) Health Information Management Journal 14

Burns, Kara and Suzanna Belton, ‘”Click First, Care Second” Photography’ 2012 197(5) Medical Journal of Australia 265

Burns, Kara and Suzanna Belton, ‘Clinicians and their Cameras: Policy, Ethics and Practice in an Australian Tertiary Hospital’ 2013 37 Australian Health Review 437

Carruth, Kristen A and Harvey J Ginsburg, ‘Social Networking and Privacy Attitudes Among College Students’ 2014 6(2) *Psychology, Education & Society* 82

Chretien, Katherine C and Terry Kind, ‘Social Media and Clinical Care: Ethical, Professional, and Social Implications’ 2013 127(13) *Circulation* 1413


Cruess, Richard and Sylvia Cruess, ‘Updating the Hippocratic Oath to Include Medicine’s Social Contract’ 2014 48 *Medical Education* 95


Hill, Kate, ‘Consent, Confidentiality and Record Keeping for Recording and Usage of Medical Images’ 2006 29(2) *Journal of Visual Communications in Medicine* 76


Jones, Bolette, ‘“Drop ‘em Blossom” – Clinical Photography and Patient Dignity’ 1996 19(2) *Journal of Audiovisual Media in Medicine* 85

Jonsen, Albert, *Short History of Medical Ethics* (Oxford University Press, 2000) 100

Ke, Malcolm, Danielle Moul, Melissa Camouse, Mathew Avram, Dafnis Carranza, Teresa Soriano and Gary Lask ‘Where is it? The Utility of Biopsy Site Photography’ 2010 36(2) *Dermatologic Surgery* 198
Kelly, John B, and Hanspaul S Makkar, ‘Ethics in Pediatric Dermatology’ 2012 30 Clinics in Dermatology 471

Kerridge, Ian, Michael Lowe and John McPhee, Ethics and Law for the Health Professions (The Federation Press, 2nd ed, 2005)

Kirk, Michael, Sarah Hunter-Smith, Katrina Smith and David Hunter-Smith, ‘The Role of Smartphones in the Recording and Dissemination of Medical Images’ 2014 3(2) Journal of Mobile Technology in Medicine 40


Kunde, Lauren, Erin McMeniman and Malcolm Parker, ‘Clinical Photography in Dermatology: Ethical and Medico-legal Considerations in the Age of Digital and Smartphone Technology’ 2013 54 Australasian Journal of Dermatology 192

Lakdawala, Nikita, Demian Fontanella and Jane Grant-Kels, ‘Ethical Considerations in Dermatologic Photography’ 2012 30 Clinics of Dermatology 486


Lockwood, Gillian, ‘Confidentiality’ 2007 3(3) The Foundation Years 107
Luo, John, Christopher Logan, Thomas Long and Lionel Bercovitch, ‘Cyberdermatoethics I: Ethical, Legal, Technologic, and Clinical Aspects of Patient-Physician e-mail’ 2009 27Clinics in Dermatology 359


McGinness, Jamie Lynn and Glenn Goldstein, ‘The Value of Preoperative Biopsy-Site Photography for Identifying Cutaneous Lesions’ 2010 36(2) Dermatologic Surgery 194

McIlwraith, Janine and Bill Madden, Health Care & the Law (Thomson Reuters (Professional) Australia Limited, 5th ed, 2010)

McMillen, David, ‘Privacy, Confidentiality, and Data Sharing: Issues and Distinctions’ 2004 21 Government Information Quarterly 359


Palacios-González, César, ‘The Ethics of Clinical Photography and Social Media’ 2015 18 Medical Health Care and Philosophy 63


Percival, Thomas, Medical Ethics: or, a Code of Institutes and Precepts, Adapted to the Professional Conduct of Physicians and Surgeons (London: W Jackson, 1803) 390

Purtilo, Ruth, Ethical Dimensions in the Health Profession (Elsevier Saunders, 5th ed, 2005)
Ratner, Désirée, Craig Thomas and David Bickers, ‘The Uses of Digital Photography in Dermatology’ 1999 41(7) *Journal of American Dermatology* 49

Rinehart-Thompson, Laurie A, Beth M Hjort and Bonnie S Cassidy, ‘Redefining the Health Information Management Privacy and Security Role’ 2009 6 *Perspectives in Health Information Management* 1


Robinson, June, Ashish Bhatia and Jeffrey Callen, ‘Protection of Patients’ Right to Privacy in Clinical Photographs, Video, and Detailed Case Descriptions’ 2014 150(1) *Journal of American Medical Association Dermatology* 14


Scott, Graham, ‘Social Media is Blurring Professional Boundaries’ 2013 27(52) *Nursing Standard* 1


Srinivasan, S, ‘Compromises in Healthcare Privacy due to Data Breaches’ 2016 4 *European Scientific Journal* 91


Swick, Herbert, Philip Szenas, Deborah Danoff and Michael Whitcomb, ‘Teaching Professionalism in Undergraduate Medical Education’ 1999 282(9) *Journal of American Medical Association* 830


Tomlinson, Jillian, Andrew Myers and Bryce Mead, “‘Click First, Care Second’ Photography: To the Editor’ 2013 198(1) *Medical Journal of Australia* 21

Twenge, Jean M, Sara Konrath, Joshua D Foster, W Keith Campbell and Brad J Bushman, ‘Egos Inflating Over Time: A Cross-Temporal Meta-Analysis of the Narcissistic Personality Inventory’ 2008 76(4) *Journal of Personality* 875

United States Federal Government, ‘Modification of the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology and Economic and Clinical Health Act and the Genetic Information Non-discrimination Act; Other Modifications to the HIPAA Rules; Final Rule’ 2013 78(17) *Federal Register* 5566

van der Heijden, J, N Keizer, J Bos, P Spuls and L Witkamp, ‘Teledermatology Applied Following Patient Selection by General Practitioners in Daily Practice Improves Efficiency and Quality of Care at Lower Cost’ 2011 165 *British Journal of Dermatology* 1058

Van der Rijt, Rhys and Stuart Hoffman, ‘Ethical Considerations of Clinical Photography in an Area of Emerging Technology and Smartphones’ 2014 40 *Journal of Medical Ethics* 211


**B Cases**

*Anderson v Mayo Clinic* 2008 WL 3836744 (Minn. App.)

*Attorney General v Guardian Newspapers Ltd (No. 2)* [1988] 3 All ER 545

*Brown v Brooks* (Unreported, Supreme Court of New South Wales, McLelland J, 18 August 1988)

*Coco v AN Clark (Engineers) Ltd* [1969] RPC 41

*Davis and Barking, Havering and Brentwood Health Authority* (1993) 4 Med LR 85

*Donoghue v Stevenson* [1932] AC 562

*F v West Berkshire Health Authority* [1989] 2 All ER 545

*Grosse v Purvis* [2003] QDC 151

‘IV’ and ‘IW’ [2016] AlCmr 41 (27 June 2016)

*Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281
John Fairfax Publications Pty Ltd v Hitchcock [2007] NSWCA 364 [123]

KJ v Wentworth Area Health Service [2004] NSWADT 84

Murray v McMurchy [1949] 2 DLR 442

O’Brien v Cunard Steamship Co. (1891) 28 NE 266

Re C (Adult: Refusal of Medical Treatment) [1994] 1 WLR 290

Re T (Adult: Refusal of Treatment) [1993] Fam 95

Richards v Kadian [2008] NSWCA 328

Rogers v Whitaker (1992) 175 CLR 479

Schloendorf v Society of New York Hospital, 195 NE 92 (NY, 1914)

Secretary, Department of Health and Community Services (NT) v JWB (Marion’s case) (1992) 175 CLR 218

Tarasoff v The Regents of the University of California 551 P2d 334 (Cal 1976)

Victoria Park Racing and Recreation Grounds Company Limited v Taylor (1937) 58 CLR 479

W v Edgell [1990] 1 All ER 855

Wyong Shire Council v Shirt (1980) 146 CLR 40

C Legislation
An Act to define the qualifications of Medical Witnesses at Coroners’ Inquests and Inquires held before Justices of the Peace in the Colony of New South Wales 1883 (NSW) (2 Victoria, Act No 22)

*Australian Constitution 1901* (Cth)

*Australian Information Commissioner Act 2010* (Cth)

*Crimes Act 1914* (Cth)

*Freedom of Information Act 1982* (Cth)


*Health Practitioner Regulation National Law Act 2010* (ACT)

*Health Practitioner (National Uniform Legislation) Implementation Act 2012* (NT)

*Health Practitioner Regulation (Adoption of National Law) Act 2009* (NSW)

*Health Practitioner Regulation National Law Act 2009* (Qld)

*Health Practitioner Regulation National Law (South Australia) Act 2010* (SA)

*Health Practitioner Regulation National Law (Tasmania) Act 2010* (Tas)

*Health Practitioner Regulation National Law (Victoria) Act 2009* (Vic)

*Health Practitioner Regulation National Law (Western Australia) Act 2010* (WA)

*Healthcare Identifiers Act 2010* (Cth)

*Medical Act 1858* (UK)

*Medical Ordinance Act 1869* (WA)
Privacy Act 1988 (Cth)

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)

Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) Explanatory Memorandum

Privacy Amendment (Notification of Serious Data Breaches) Bill 2016 (Cth) Explanatory Memorandum

42 USC §§ 1320d–1320d (2009)

42 USC §§ 17931–17940 (2009)

D Treaties


E Other

A Better NHS, Medical Power (5 October 2012) <https://abetternhs.net/2012/10/05/medical-power/>


Australian Medical Association, *Use and Disclosure of Clinical Images*  

Australian Red Cross Blood Service, *Blood Service Apologies for Donor Data Leak*  

Barbaro, Michael and Tom Zellar, *A Face is Exposed for AOL Searcher 4417749*  
(9 August 2006) New York Times  

Birch, Jim and Shelly Park, *A Note From the Blood Service Chief Executive and the Chair*  

Centre for Internet Safety, University of Canberra, Privacy and the Internet: Australian Attitudes Towards Privacy in the Online Environment  

Croucher, Rosalind, ‘President of the Australian Law Reform Commission’ (Speech delivered at the Managing Patient Confidentiality & Information Governance Forum, Melbourne, 22 August 2011)

Department of Health, Australian Government, MBS Online Medical Benefits Schedule, *The July 2016 Medical Benefits Schedule*, s G15.1  

Department of Health, Australian Government, *National Registration and Accreditation Scheme (NRSA)*  

Department of Health and Human Services, *Data Breach Results in $4.8 million HIPAA Settlement* (7 May 2014)  
Department of Health and Human Services, $4.8 million HIPAA Settlement Underscores Importance of Managing Security Risks (18 October 2016)

Explanatory Memorandum, Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Cth)


MacGibbons, Alastair and Nigel Phair, *Privacy and the Internet: Australian Attitudes Towards Privacy in the Online Environment* (2012) Centre for Internet Safety – University of Canberra Law Faculty

McGilvray, Annabel, *Medical Journal of Australia: Online Security*  


MDA National, *Medical Records*  


Medical Board of Australia, *Good Medical Practice: A Code of Conduct for Doctors in Australia* (2014)

Medical Board of Australia, *Interns: Registration Standard – Granting General Registration as a Medical Practitioner to Australian and New Zealand Medical Graduates on Completion of Intern Training*  
<http://www.medicalboard.gov.au/documents/default.aspx?record=WD12%2f9504%5bv2%5d&dbid=AP&chksum=PvYzX0nEOt%2bYT0wNVghlkA%3d%3d>

Medical Board of Australia, *Medical Board Consults on Revalidation in Australia*  

Medical Board of Australia, *Medical Board of Australia Registrant Data – Reporting Period: October 2015 – December 2015* (2016) AHPRA  

Melbourne Pathology, *Online Results* (2016)


National Nurse, *HIPAA – The Health Insurance Portability and Accountability Act: What RNs Need to Know About Privacy Rules and Protected Electronic Health Information* <http://nurses.3cdn.net/9480c5f5520f52a8e5_vsm6bp9vu.pdf>


OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*  
<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>

Office of the Australian Information Commissioner, Australian Government,  

Office of the Australian Information Commissioner, Australian Government,  


Pharmacology and Therapeutics Panel Discussion (Created by Colby Evans, Jeffrey Callen, Whitney High, Derm Cast TV, 04 December 2015)


Privy Council Office, Chartered Bodies <https://privycouncil.independent.gov.uk/royal-charters/chartered-bodies/>

RACGP, Certificate of Primary Care Dermatology <http://www.racgp.org.au/education/courses/dermatology/>


Royal College of General Practitioners, *Guide for the Use of Social Media in General Practice* (2015)


<http://www.wma.net/en/30publications/10policies/g1/>