

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

SCARLETTE DE LAVAINÉ

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
	<i>A Overview of this Thesis Paper</i>	<i>1</i>
	<i>B Outline of this Thesis Paper</i>	<i>6</i>
II	PRIVACY, CONFIDENTIALITY AND CONSENT.....	8
	<i>A The Importance of Privacy, Confidentiality and Consent</i>	<i>9</i>
III	PRIVACY PROBLEMS WITH DIGITAL PHOTOGRAPHY IN HEALTHCARE	15
	<i>A Digital Photography, Electronic Medical Records and the Law</i>	<i>15</i>
	<i>B Issues of Consent and Record Keeping</i>	<i>19</i>
	<i>C The Issue of Identifiability</i>	<i>24</i>
	<i>D Portable Devices and Clinical Photography.....</i>	<i>27</i>
	<i>E Security Issues of Digital Clinical Photography</i>	<i>29</i>
	<i>F Loss of Control – ‘Information Drift’</i>	<i>33</i>
	<i>G The Effects of Social Media on Attitudes Towards Privacy</i>	<i>34</i>
IV	REGULATORY BODIES AND CODES OF CONDUCT.....	37
	<i>A The Introduction of the Modern Professional Code.....</i>	<i>37</i>
	<i>B The Role of Professional Codes in Healthcare Regulation.....</i>	<i>38</i>
	<i>C Confidentiality and Professional Codes</i>	<i>40</i>
	<i>D The Australian Health Practitioner Regulation Agency (AHPRA)</i>	<i>42</i>
	<i>E The Medical Board of Australia (MBA)</i>	<i>43</i>
	<i>F The Royal Australian College of General Practitioners (RACGP).....</i>	<i>44</i>
	1 <i>An Overview of the RACGP</i>	<i>44</i>
	2 <i>RACGP ‘Standards for General Practice’</i>	<i>45</i>
	3 <i>RACGP Guidelines – What is Missing?.....</i>	<i>46</i>
	<i>G The Australian Medical Association (AMA).....</i>	<i>47</i>
V	FEDERAL PRIVACY LEGISLATION	50
	<i>A Background of the Privacy Act 1988 (Cth).....</i>	<i>51</i>
	<i>B The Australian Law Reform Commission: Report 108.....</i>	<i>52</i>
	<i>C The Privacy Amendment (Enhancing Privacy Protection) Act 2012</i>	<i>53</i>
	1 <i>Australian Privacy Principles (APPs)</i>	<i>56</i>

2	<i>Breach of the Privacy Act</i>	64
VI	CONCLUSION	72
	<i>A The Problem Re-visited</i>	72
	<i>B Increased Education - A Proactive Approach</i>	72
	<i>C Indoctrination of Hospital-based Junior Doctors</i>	74
	<i>D Continuing Professional Development Training</i>	75
	<i>E Final Comments</i>	76
VII	ANNEXURES	79
	<i>Annexure A</i>	79
	<i>Annexure B</i>	80
VIII	GLOSSARY OF TERMS	81
IX	ACRONYMS	85
X	BIBLIOGRAPHY	87
	<i>A Articles/Books/Reports</i>	87
	<i>B Cases</i>	94
	<i>C Legislation</i>	95
	<i>D Treaties</i>	97
	<i>E Other</i>	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

¹ Kara Burns and Suzanna Belton, “Click First, Care Second” Photography’ 2012 197(5) *Medical Journal of Australia* 265, 265; Scheinfeld et al, ‘Trends in the Use of Cameras and Computer Technology Among Dermatologists in New York City 2001–2002’ 2003 29(8) *Dermatologic Surgery* 822, 822.

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 disseminated⁷ 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

² Nikita Lakdawala, Demian Fontanella and Jane Grant-Kels, 'Ethical Considerations in Dermatologic Photography' 2012 30 *Clinics of Dermatology* 486, 486; Cunniff et al, 'Informed Consent for Medical Photographs' 2000 2(6) *Genetics in Medicine* 353, 353.

³ Désirée Ratner, Craig Thomas and David Bickers, 'The Uses of Digital Photography in Dermatology' 1999 41(7) *Journal of the American Dermatology* 49, 49; Cunniff et al, above n 2, 353.

⁴ Paul Stevenson, Anna Finnane and Peter Soyer, 'Teledermatology and Clinical Photography: Safeguarding Patient Privacy and Mitigating Medico-legal Risk' 2016 204(5) *Medical Journal of Australia* 198, 198.

⁵ Burns and Belton, above n 1, 265.

⁶ Rachel Kornhaber, Vasilki Betihavas and Rodney Baber, 'Ethical Implications of Digital Images for Teaching and Learning Purpose: An Integrative Review' 2015 8 *Journal of Multidisciplinary Healthcare* 299, 301; Kara Burns, 'Smartphones in Medicine Need to be Smarter' 2013 3(3) *Health Information Management Journal* 14, 14; Rhys Van der Rijt and Stuart Hoffman, 'Ethical Considerations of Clinical Photography in an Area of Emerging Technology and Smartphones' 2014 40 *Journal of Medical Ethics* 211, 212.

⁷ Patricia Sánchez Abril, Avner Levin and Alissa Del Riego, 'Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee' 2012 49(1) *American Business Law Journal* 63, 64.

⁸ Stevenson, Finnane and Soyer, above n 4, 198.

professional.⁹ The boundary between professional and personal network use is fluid.¹⁰ 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,¹¹ cosmetic surgery,¹² burns and wound care.¹³ Providing a visual record, digital photographs aid diagnosis, monitor change and quantify response to therapy.¹⁴ 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.¹⁵ 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/9480c5f5520f52a8e5_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 Tele dermatology: A Case Study' (2014) 7 *BioMed Central Research Notes* 588, 588.

¹² M Harting, J DeWees and K Vela, R Khirallah, 'Medical Photography: Current Technology, Evolving Issues and Legal Perspectives' 2015 69 *International Journal of Clinical Practice* 401, 402.

¹³ Van der Rijt and Hoffman, above n 6, 211.

¹⁴ Ibid.

¹⁵ Scheinfeld et al, above n 1, 822.

digital photography¹⁶ by medical practitioners.¹⁷ Directly or with adapters,¹⁸ smart phone cameras can capture images, which can be uploaded into patient records or emailed to an authority for advice.¹⁹ The simplicity and familiarity of the process facilitates the addition of clinical pictures.²⁰

Medical practitioners²¹ are legally required to maintain patient privacy and confidentiality.²² Identifiable clinical photographs form part of a patient's medical record and therefore, attract the same protection as a written record.²³ Collection, use and disclosure *require patient consent*.²⁴ 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.²⁵ It is a controlling condition.²⁶ 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.²⁷

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.²⁸ 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.

¹⁶ This paper uses the terms 'digital photography', 'clinical photography' and 'digital images' interchangeably.

¹⁷ Burns and Belton, above n 1, 265; Mahar et al, 'Legal Considerations of Consent and Privacy in the Context of Clinical Photography in Australian Medical Practice' 2013 198(1) *Medical Journal of Australia* 48, 48.

¹⁸ For example, the 'Mole Scope' iPhone adapter \$99 USD; MoleScope, *Products* <<https://molescope.com/product/>>.

¹⁹ Stevenson, Finnane and Soyer, above n 4, 198.

²⁰ Kornhaber, Betihavas and Baber, above n 6, 299-300; Colton Nielson, Cameron West and Ikue Shimizu, 'Review of Digital Image Security in Dermatology' 2015 21(10) *Dermatology Online Journal* 1, 1-2.

²¹ This paper uses the terms 'medical practitioner', 'practitioner' and 'doctor' interchangeably.

²² Privacy Act 1988 (Cth) sch 1 pt 3 sub-cl 6.1; Health Practitioner Regulation National Law (WA) Act 2010 (WA) sch pt 5 s 40.

²³ 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.

²⁴ *Privacy Act 1988* (Cth) sch 1 pt 3 cl 6.

²⁵ Ibid.

²⁶ Medical Board of Australia, *Practice: A Code of Conduct for Doctors in Australia* (March 2014) Australian Health Practitioner Regulation Agency <<http://www.medicalboard.gov.au/Codes-Guidelines-Policies/Code-of-conduct.aspx>>.

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.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.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'.³¹ The legal obligations are clearly described in the Medical Board of Australia's Code,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 AHPRA³³ 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.

²⁹ Ibid 2.

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.

³¹ Louis Lasagna, 'Modern Hippocratic Oath' 1995 72(11) *Medical Economics* 202, 202.

³² Medical Board of Australia, above n 26; RACGP, *Standards for General Practices 4th ed criterion 4.2.1* <<http://www.racgp.org.au/download/documents/Standards/standards4thedition.pdf>>.

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.³⁴

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').³⁵ 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.³⁶ 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.³⁷ 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

³⁴ Office of the Australian Information Commissioner, Australian Government, *Assessments* <<https://www.oaic.gov.au/privacy-law/assessments/>>.

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).

³⁷ Peter Guffin, 'Data Security Breach Notification Requirements in the United States: What You Need to Know' 2011 4 *The Quarterly Journal of PRISM International* 6, 6-12.

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.³⁸ Privacy refers to an individual's right to control of his or her own personal information.³⁹ 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.⁴⁰ 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.⁴¹

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.⁴²

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.⁴³ The

³⁸ Ian Kerridge, Michael Lowe and John McPhee, *Ethics and Law for the Health Professions* (The Federation Press, 2nd ed, 2005) 244.

³⁹ Janine McIlwraith and Bill Madden, *Health Care & the Law* (Thomson Reuters (Professional) Australia Limited, 5th ed, 2010) 276.

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; Dhair 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’⁴⁴ 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.⁴⁵ Private information may be intimate or embarrassing yet essential to receiving appropriate care.⁴⁶ The patient’s decision to reveal this information relies upon his or her freely given consent.⁴⁷ The *a priori* need for this consent arises from the ‘respect for patient autonomy... a fundamental principle in contemporary bioethics’⁴⁸ 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’.⁴⁹ 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.⁵⁰ 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.⁵¹ This grant of consent

⁴⁴ Ibid.

⁴⁵ Gillian Lockwood, ‘Confidentiality’ 2007 3(3) *The Foundation Years* 107, 107; Kerridge, Lowe and McPhee, above n 38, 227; New London Consulting, *Australia: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* (28 February 2012) Fair Warning <http://www.fairwarning.com/wp-content/uploads/2015/09/2012-04-WP-AUSTRALIA-PATIENT-SURVEY1.pdf?utm_source=survey&utm_medium=www.fairwarning.com&utm_term=australia+patient+privacy+survey&utm_content=australia+patient+privacy+survey&utm_campaign=website+content>.

⁴⁶ Kerridge, Lowe and McPhee, above n 38, 219.

⁴⁷ Ian Berle, ‘Privacy and Confidentiality: What is the Difference?’ 2011 34(1) *Journal of Visual Communication* 43, 43; Ian Berle, ‘Clinical Photography and Patients’ Rights: The Need for Orthopraxy’ 2008 34 *Journal of Medical Ethics* 89, 90.

⁴⁸ J A M De Roubaix, ‘Beneficence, Non-Maleficence, Distributive Justice and Respect for Patient Autonomy Reconcilable Ends in Aesthetic Surgery?’ 2011 64 *Journal of Plastic, Reconstructive & Aesthetic Surgery* 11, 11.

⁴⁹ Tom Beauchamp and James Childress, *Principles of Biomedical Ethics* (Oxford University Press, 6th ed 2009) 99.

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'⁵² physicians⁵³ 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.'⁵⁴

Private information that is communicated by the patient to the medical practitioner is protected by *confidentiality*.⁵⁵ 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'.⁵⁶ 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.⁵⁷ This principle of 'secondary' disclosure is recognised in APP 6. If 'the individual would *reasonably expect*' that disclosure supports the '*primary purpose*'⁵⁸ 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'.⁵⁹

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.

⁵⁵ Abraham Schwab, Lily Frank and Nada Gligorov, 'Saying Privacy, Meaning Confidentiality' 2011 11(11) *The American Journal of Bioethics* 44, 45; For the 'Duty of Confidentiality' see *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 [47].

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.⁶⁰ The majority of patients appreciate the need to balance these tensions, accepting this type of disclosure appropriate in the context of clinical photographs.⁶¹ 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 patient⁶² and he or she must have the legal capacity⁶³ to understand what is being consented to, including the benefits, risks,⁶⁴ likely outcome, and in some cases, possible alternatives.⁶⁵ 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.⁶⁶ Additionally, the consent must be specific, that is, consent must be given to a specific act or treatment⁶⁷ and cannot be a 'blanket' agreement,⁶⁸ and it must be granted freely and without coercion.⁶⁹ 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.⁷⁰ Although patients may withdraw consent at any time,⁷¹ it is essential the patient understands that once images have entered the public domain the images are likely irretrievable.⁷²

⁶⁰ Ibid sch 1 pt 3 cl 6.

⁶¹ Catherine Lau, Hagan Schumacher and Michael Irwin, 'Patients' Perception of Medical Photography' 2010 63 *Journal of Plastic, Reconstructive & Aesthetic Surgery* e507, e508.

⁶² *Rogers v Whitaker* (1992) 175 CLR 479.

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 McMurchy* [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.

⁷⁰ Australian Medical Association, Privacy and Health Record Resource Handbook: For Medical Practitioners in the Private Sector (2014) 21; Taylor et al, 'A Study of the Personal Use of Photography within Plastic Surgery' 2008 61 *Journal of Plastic, Reconstructive & Aesthetic Surgery* 37, 39.

⁷¹ Kerridge, Lowe and McPhee, above n 38, 354; Franchitto et al, 'Photographs, Patient Consent and Scientific Publications: Medicolegal aspects in France' 2008 15 *Journal of Forensic and Legal Medicine* 210, 211.

⁷² Lakdawala, Fontanella and Grant-Kels, above n 2, 488; Kornhaber, Betihavas and Baber, above n 6, 301; Payne et al, 'A Review of Current Clinical Photography Guidelines in Relation to Smartphones Publishing of Medical Images' 2012 35(4) *Journal of Visual Communication in Medicine* 188, 189.

Despite the importance consent plays in respecting patient autonomy and confidentiality, often insufficient attention is given to the process of obtaining patient consent.⁷³ Clinical photography may leave an already vulnerable patient feeling objectified if their right to autonomy is disrespected.⁷⁴ Still, it is not uncommon for practitioners to rely on implied consent for clinical photography.⁷⁵ As implied consent is not defined, it may be open to interpretational discrepancies between patient and practitioner.⁷⁶ 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.⁷⁷ 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'⁷⁸ (for example, to seek diagnostic assistance from a colleague).⁷⁹ 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.⁸⁰

The power structure of the doctor-patient relationship is widely acknowledged to be unequal.⁸¹ 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

⁷³ Michael Davis, 'Safeguarding Patient Privacy in the Context of Clinical Innovation' 2014 1 *Australian Health Law Bulletin* 117, 119; Noah Scheinfeld and Brooke Rothstein, 'HIPAA, Dermatology Images, and the Law' 2013 32 *Seminars in Cutaneous Medicine and Surgery* 199, 199.

⁷⁴ Berle, above n 47, 43; Berle, above n 47, 90; Bolette Jones, "'Drop 'em Blossom' – Clinical Photography and Patient Dignity' 1996 19(2) *Journal of Audiovisual Media in Medicine* 85, 85.

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 Baber, 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.

⁷⁹ Australian Medical Association, *Clinical Images and the use of Personal Mobile Devices* <https://ama.com.au/sites/default/files/FINAL_AMA_Clinical_Images_Guide_0.pdf>.

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 patient⁸² may accept personally unpalatable behaviour if refusal to comply is felt to be either impossible or counterproductive to receiving the best care,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’.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.⁸⁵ The right to retain control over private information requires confidentiality.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.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.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.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’.⁹⁰ Thomas Percival, an English physician at the beginning of the 19th century, has been recognised as drafting the first modern (medical) professional code of ethics.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

⁸² Berle, above n 47, 43; Berle, above n 47, 90.

⁸³ Burns and Belton, above n 1, 265; Berle, above n 47, 90.

⁸⁴ Berle, above n 47, 90.

⁸⁵ Amaboo and Payne-James, above n 41, 60.

⁸⁶ Lockwood, above n 45, 107.

⁸⁷ Gerald Higgins, ‘The History of Confidentiality in Medicine: The Physician-Patient Relationship’ 1989 35 *Canadian Family Physician* 921, 922.

⁸⁸ *Ibid.*

⁸⁹ Lisa Napoli, ‘The Doctrine of Informed Consent and Women: The Achievement of Equal Value and Equal Exercise of Autonomy’ 1996 4 *Journal of Gender & the Law* 335, 335, 338-339, 349-350.

⁹⁰ Lockwood, above n 45, 107.

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.

⁹³ Jeffrey Berlant, ‘Profession and Monopoly: A study of medicine in the United States and Great Britain’ 1976 20(3) *Medical History* 342, 342.

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.⁹⁴ Unlike financial account details, stolen health information cannot be replaced for uncompromised data.⁹⁵ An estimated 7.5% of patients in the United States will fall victim to personal healthcare data theft within the next 5 years.⁹⁶ One third of all data breaches reported in 2015 occurred in the health/medical sector.⁹⁷ Mandatory reporting of breach incidents has led to more litigation suits and successively heavier regulatory fines.⁹⁸

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'.⁹⁹ 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.¹⁰⁰ The 'Privacy Amendment (Notification of Serious Data Breaches) Bill 2016 (Cth) is due before Parliament in the Spring 2016 sitting.¹⁰¹ 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

⁹⁴ Annabel McGilvray, *Medical Journal of Australia: Online Security* <<https://www.mja.com.au/careers/198/3/online-security>>.

⁹⁵ S Srinivasan, 'Compromises in Healthcare Privacy due to Data Breaches' 2016 4 *European Scientific Journal* 91, 93; Samantha Pillay, *Mandatory Data Breach Notification – What does it mean for Healthcare Providers?* (21 September 2016) Lexology Associate Corporate Counsel Australia <http://www.lexology.com/library/detail.aspx?g=5d0acc25-35e2-462c-bb31-f78495b23972&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Australian+IHL+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2016-10-04&utm_term=>>.

⁹⁶ Pillay, above n 95.

⁹⁷ The Identity Theft Centre, *Identity Theft Resource Centre Breach Report Hits Near Record High in 2015* <<http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html>>.

⁹⁸ Paul Smith, 'Litigation, PR Disasters and Higher Insurance Costs Expected From New Data Breach Laws' *Australian Financial Review (Online)*, 10 August 2015 <<http://www.afr.com/technology/litigation-pr-disasters-and-higher-insurance-expected-from-new-data-breach-laws-20150805-gis75j>>.

⁹⁹ Ruth Liew, 'Top Australian Cyber Crime Targets for 2016 named' *Australian Financial Review (online)*, 24 November 2015 <<http://www.afr.com/technology/top-australian-cyber-crime-targets-for-2016-named-20151120-gl40zk>>.

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.¹⁰²

Unlike the US and Canada,¹⁰³ Australia does not recognise tortious invasion of privacy.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.¹⁰⁵ Several definitions in the Act have been updated: Clinical photographs, which form part of a patient's medical record,¹⁰⁶ are 'health information'.¹⁰⁷ *Health information* is now recognised as 'sensitive information' by the Federal public sector,¹⁰⁸ affording it increased protection.¹⁰⁹

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

¹⁰² See Ch 5, 'Breach of the Privacy Act' of this paper.

¹⁰³ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) vol 1, 126.

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.

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.

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>>.

¹⁰⁷ *Privacy Act 1988* (Cth) s 6FA(b) defines 'health information' as 'other personal information collected to provide, or in providing, a health service'.

¹⁰⁸ *Privacy Act 1988* (Cth) s 6 defines 'sensitive information' which includes 'health information'; Australian Medical Association, above n 79.

¹⁰⁹ *Privacy Act 1988* (Cth) ss 6(1), sch 1 pt 2 sub-cl 3.3–3.4, sch 1 pt 2 sub-cl 6.2.

¹¹⁰ *Privacy Act 1988* (Cth) ss 13G, 80W.

¹¹¹ Kornhaber, Betihavas and Baber, above n 6, 301; Burns, above n 6, 14; Van der Rijt and Hoffman, above n 6, 212.

¹¹² F Jamil, 'Smartphone Photography Oral and Maxillofacial Surgery' 2016 54 *British journal of Oral and Maxillofacial Surgery* 104, 105.

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.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.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.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.¹¹⁷ The longer the delay between biopsy and full excision, the higher the chance of incorrect site identification,¹¹⁸ a frequent cause of medico-legal lawsuits.¹¹⁹ Erroneous site identification in one survey was a reported 14%.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.¹²¹

Clinical photography, when used within the constraints of the law, offers a practical, effective solution to identify the correct site,¹²² protecting practitioners from lawsuits.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.¹²⁴ Depending on the lesion's placement, the photograph frame may

¹¹⁴ Stevenson, Finnane and Soyer, above n 4, 198.

¹¹⁵ Comfere et al, 'Provider-to-Provider Communications in Dermatology and Implications of Missing Clinical Information in Skin Biopsy Requisition Forms: A Systematic Review' 2014 53 *International Journal of Dermatology* 549, 549; *Pharmacology and Therapeutics Panel Discussion* (Created by Colby Evans, Jeffrey Callen, Whitney High, Derm Cast TV, 04 December 2015) 00:12:50 <<http://dermcast.tv/pharmacology-and-therapeutics-panel-discussion-colby-evans-md-jeffrey-callen-mdand-whitney-high-md/>>.

¹¹⁶ Comfere et al, above n 115, 549.

¹¹⁷ Jamie Lynn McGinness and Glenn Goldstein, 'The Value of Preoperative Biopsy-Site Photography for Identifying Cutaneous Lesions' 2010 36(2) *Dermatologic Surgery* 194, 197; *Pharmacology and Therapeutics Panel Discussion*, above n 115, 00:21:48.

¹¹⁸ McGinness and Goldstein, above n 117, 195.

¹¹⁹ Ke et al, 'Where Is it? The Utility of Biopsy Site Photography' 2010 36(2) *Dermatologic Surgery* 198, 198.

¹²⁰ *Ibid* 198.

¹²¹ McGinness and Goldstein, above n 117, 195.

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.

¹²³ McGinness and Goldstein, above n 117, 197.

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.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.¹²⁶ A physical skin examination of the entire body can be used to identify skin lesions that may present a risk of malignancy,¹²⁷ and can be supplemented with photographic documentation to assist with 'anatomically correct mapping'.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.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.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,¹³¹ has simplified widespread use of digital photography within medicine.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.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,¹³⁴ and documentation was poor - only 23% recorded consent in the medical records.¹³⁵ In another Australian study, all of the participating medical registrars used their phones to photograph patients.¹³⁶

¹²⁵ Ibid; Pharmacology and Therapeutics Panel Discussion, above n 115, 00:15:51.

¹²⁶ Scheinfeld and Rothstein, above n 73, 199.

¹²⁷ Risser et al, 'The Impact of Total Body Photography on Biopsy Rate in Patients from a Pigmented Lesion Clinic' 2007 57(3) *Journal of the American Academy of Dermatology* 428, 429.

¹²⁸ Jin et al, 'Surgical Pearl: The use of Polaroid Photography for Mapping Mohs Surgery Sections' 2005 52 *Journal of the American Academy of Dermatology* 511, 511.

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.

¹³⁸ Kara Burns and Suzanna Belton, ‘Clinicians and their Cameras: Policy, Ethics and Practice in an Australian Tertiary Hospital’ 2013 37 *Australian Health Review* 437, 437-8; V Hubbard, D Goodard and S Walker, ‘An Online Survey of the Use of Digital cameras by Members of the British Association of Dermatologists’ 2009 34 *Clinical and Experimental Dermatology* 492, 492.

¹³⁹ *Schloendorff 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); *Schloendorff v Society of New York Hospital*, 195 NE 92 (NY, 1914); Hood, Hope and Dove, above n 23, 1009.

¹⁴¹ Martin Johns ‘Informed Consent for Clinical Photographs’ 2002 25(2) *Journal of Audiovisual Media in Medicine* 59, 59.

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.¹⁴⁶ Like tiny pieces of a large jigsaw puzzle, an identifiable picture of an individual may be assembled.¹⁴⁷ What is not ‘reasonably identifiable’ today may become so in the future.¹⁴⁸ Will the courts’ understanding of ‘reasonableness’ change when it relates to ‘identifiable’?

The Privacy Act does not apply to de-identified information.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’.¹⁵⁰ Under the Privacy Act, ‘health information’ is information ‘collected to provide, or in providing, a ‘health service’¹⁵¹ to an individual’ only if the information falls within the meaning of ‘personal information’.¹⁵²

Use of a de-identified photograph originally taken during the provision of a health service would not, *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 *recognisable content* or *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’

¹⁴⁶ Susan Krashinsky, *Google Broke Canada’s Privacy Laws with Targeted Health Ads, Watchdog Says* (15 January 2014) The Globe and Mail
<<http://license.icopyright.net/user/viewFreeUse.act?fuid=MjM5MjExODg%3D>>.

¹⁴⁷ For example internet provider AOL released de-identified internet searches (which included searches for health related information) and a few days later the *New York Times* published an article reporting that they had successfully re-identified customers based on the search data: Michael Barbaro and Tom Zellar, *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>.

¹⁴⁸ This was an issue raised in the ALRC report, concerning biometric ID, such as facial recognition; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) vol 1, 322–3.

¹⁴⁹ See, de-identified information does not meet the definition of ‘personal information’; *Privacy Act 1988* (Cth) s 6(1) ‘personal identification’.

¹⁵⁰ *Ibid* sch 1 pt 2 sub-cl 3.3(a)(i).

¹⁵¹ *Ibid* s 6FB ‘health service’.

¹⁵² *Ibid* s 6FA(b) ‘health information’.

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.

¹⁵⁵ AHPRA, *Possible Outcomes* (2016) <<http://www.ahpra.gov.au/Notifications/Find-out-about-the-complaints-process/Possible-outcomes.aspx>>.

¹⁵⁶ Royal College of General Practitioners, *Handbook for the Management of Health Information in General Practice* 3rd ed (2016) 4.

¹⁵⁷ *O'Brien v Cunard Steamship Co.* (1891) 28 NE 266 cited by Marc Stauch, Kay Wheat and John Tingle, *Text, Cases & Material on Medical Law* (Routledge Cavendish, 5th ed, 2006) 102; Kunde, McMeniman and Parker, above n 75, 194.

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]lack[ing] out the eyes and face rarely achieves anonymity’.¹⁶⁵ ‘[It] 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

¹⁶⁰ Taylor et al, above n 70, 39.

¹⁶¹ *Privacy Act 1988* (Cth) sch 1 pt 3 sub-cl 6.2(a)(i); if the images is identifiable it consent must precede disclosure.

¹⁶² *Ibid*; see, eg, above n 26 (professional code of conduct).

¹⁶³ Davis, above n 73, 119.

¹⁶⁴ Taylor et al, above n 70, 39.

¹⁶⁵ *Ibid*.

¹⁶⁶ *Ibid*.

¹⁶⁷ Berle, above n 47, 43; Berle, above n 47, 90; Kornhaber, Betihavas and Baber, above n 6, 300.

¹⁶⁸ Berle, above n 47, 43; Berle, above n 47, 90; Burns and Belton, above n 1, 5.

¹⁶⁹ Berle, above n 47, 90.

¹⁷⁰ Royal College of General Practitioners, above n 156, 4; Australian Medical Association, above n 70, 21; Mahar et al, above 17, 194.

¹⁷¹ Burns and Belton, above n 138, 438; Kunde, McMeniman and Parker, above n 75, 192-4.

¹⁷² Kunde, McMeniman and Parker, above n 75, 194.

¹⁷³ Burns and Belton, above n 1, 265; Scheinfeld and Rothstein, above n 73, 199–200.

¹⁷⁴ Medical Board of Australia, above n 26.

¹⁷⁵ Van der Rijt and Hoffman, above n 6, 211.

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'.¹⁷⁶

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,¹⁷⁷ must be retained and secured for at least seven years.¹⁷⁸ During this period, they must remain accessible to the patient, if requested,¹⁷⁹ under the Freedom of Information legislation¹⁸⁰ and APP 12.¹⁸¹

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.¹⁸² 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'.¹⁸³ Unlike the Privacy Act, the Code also requires that *even non-identifiable pictures are subject to prior consent* for each and every use.¹⁸⁴ MDA National,¹⁸⁵ 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.

¹⁷⁷ Xavier Fagan, *An Annual Update for MDA National Ophthalmology Members: Imaging in Ophthalmology and How it Affects You* <<http://www.mdanational.com.au/~media/Files/MDAN-Corp/Publications/Ophthalmology-Update-2015.pdf?la=en>>; Hood, Hope and Dove, above n 23, 1009.

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.*

¹⁸⁵ See MDA National, '*MDA National*' <<http://www.mdanational.com.au/>>.

identified in [the] photograph'.¹⁸⁶ Consent should be 'clearly documented and the scope of any such consent be recorded.'¹⁸⁷

Clearly defined written consent can prevent future disputes. This was seen in the US case of *Anderson v Mayo Clinic*.¹⁸⁸ 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.¹⁸⁹

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.¹⁹⁰ Documentation of consent for all forms of use and disclosure might protect the practitioner from future medico-legal jeopardy.¹⁹¹

C *The Issue of Identifiability*

Clinical photographs enrich public awareness, facilitate research and can be invaluable clinical resources.¹⁹² Using them for these purposes are secondary to the primary purpose under the Privacy Act and the Code,¹⁹³ identifiable images may only be used if the patient grants consent.¹⁹⁴ Consent is more readily given by patients for de-identified photographs to be used for secondary purposes.¹⁹⁵ This was overwhelmingly supported by hand surgery patients.¹⁹⁶

¹⁸⁶ Yvonne Baldwin, 'Peril of the Pic' 2010 4 *First Defence MDA National* 4, 4.

¹⁸⁷ *Ibid.*

¹⁸⁸ *Anderson v Mayo Clinic*, 2008 WL 3836744 (Minn. App.)

¹⁸⁹ Jeffrey Segal and Michael Sacopolos, 'Photography Consent and Related Legal Issues' 2010 18 *Facial Plastic Surgery Clinic North America* 237, 240.

¹⁹⁰ Kate Hill, 'Consent, Confidentiality and Record Keeping for Recording and Usage of Medical Images' 2006 29(2) *Journal of Visual Communications in Medicine* 76, 76-7.

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-cl 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.¹⁹⁷ 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.¹⁹⁸ Previous methods (e.g. black-boxing and pixelating identifying regions) do not adequately de-identify people.¹⁹⁹ Patient consent for image disclosure for intended uses is preferred,²⁰⁰ a position which is supported by the International Committee of Medical Journal Editors.²⁰¹

It does, however, raise the question - when applied to the context of clinical photography, when is an image no longer considered 'reasonably identifiable'?²⁰² De-identification is not always straightforward. Unique identifiers, such as a patient's name, address or Medicare or hospital record number²⁰³ must obviously be removed. Is there an element of subjectivity,²⁰⁴ 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.²⁰⁵ Unusual anatomical or pathological features may also be identifiable.²⁰⁶

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.

¹⁹⁸ Nikita Lakdawala, Lionel Bercovitch and Jane Grant-Kels, 'Picture is Worth a Thousand Words: Ethical Dilemmas Presented by Storing Digital Photographs in Electronic Health Records' 2013 69 *Journal of the American Academy of Dermatology* 473, 473.

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.

²⁰¹ International Committee of Medical Journal Editors, *Protection of Research Participants* <<http://www.icmje.org/recommendations/browse/roles-and-responsibilities/protection-of-research-participants.html>>.

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.

²⁰³ David McMillen, 'Privacy, Confidentiality, and Data Sharing: Issues and Distinctions' 2004 21 *Government Information Quarterly* 359, 372.

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.

²⁰⁶ Office of the Australian Information Commissioner, Australian Government *What Should Health Service Providers Consider Before Taking a Photo of a Patient on a Mobile Phone?* <<https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/health-service-providers/what-should-health-service-providers-consider-before-taking-a-photo-of-a-patient-on-a-mobile-phone>>; Stevenson, Finnane and Soyer, above n 4, 200.

were leaked to the media, the patient, a male escort, sued the hospital for invasion of privacy. The action was settled out of court.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.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 dermatology²⁰⁹ 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.²¹⁰ These circumstances coupled with innate human error leaves even the most conscientious medical practitioner at risk of inadvertently saving an image incorrectly.²¹¹

²⁰⁷ Segal and Sacopulos, above n 189, 239.

²⁰⁸ See Ch III Part F ‘Loss of Control – “Information Drift”’.

²⁰⁹ For example the RACGP offers GPs the opportunity to complete a ‘Certificate of Primary Care Dermatology’ for complete details see RACGP, *Certificate of Primary Care Dermatology* <<http://www.racgp.org.au/education/courses/dermatology/>>.

²¹⁰ Pharmacology and Therapeutics Panel Discussion, above n 115, 00:18:30.

²¹¹ Ibid 00:18:50.

D *Portable Devices and Clinical Photography*

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:²¹² 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.²¹³ 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.²¹⁴ Teledermatology is the store-and-forward of images of the skin that are sent to a specialist dermatologist.²¹⁵

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 disclosure²¹⁶ or it may be insecurely transferred to the medical records or a third party.²¹⁷

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.²¹⁸

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 alphanumeric file identifier, is created at the same time as the digital photo.²¹⁹ 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

²¹² Warshaw et al, 'Teledermatology for Diagnosis and Management of Skin Conditions: A systematic Review' 2011 64(4) *Journal of American Academy of Dermatology* 759, 759.

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.²²⁰

The security risk can be recognised in the following case scenario.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%).²²² In another, 74% of doctors retained patient images, of which 32% were identifiable.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’.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.²²⁵

²²⁰ Ibid 00:23:49.

²²¹ Australian Medical Association, above n 79.

²²² Kunde, McMeniman and Parker, above n 75, 193.

²²³ Hubbard, Goodard, and Walker, above n 138, 493.

²²⁴ Burns and Belton, above n 138, 440; Richard Dean, *The Value of Humanity in Kant’s Moral Theory* (Oxford University Press, 2006).

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.²²⁶ 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.²²⁷ Violations of US federal legislation²²⁸ 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 \$250,000²²⁹ and warned of subsequent \$2.5 million fines for repeat violations.²³⁰

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.²³¹

²²⁶ Baldwin, above n 186, 4.

²²⁷ Nielson, West and Shimizu, above n 20, 2-3; Kunde, McMeniman and Parker, above n 75, 195-6.

²²⁸ Victor Gane, *Patient interaction and HIPAA compliance in our Digital World* (7 May 2014) Prime: International Journal of Aesthetic and Anti-Ageing Medicine <<https://www.prime-journal.com/patient-interaction-and-hipaa-compliance-in-our-digital-world/>>; The *Health Insurance Portability and Accountability Act 1996* (HIPAA 1996), Privacy, Security, Enforcement and Breach Notification Rules act in accordance with the *Health Information Technology for Economic and Clinical Health Act 2009* (HITECH 2009) to govern how 'personal health information' (PHI) is handled.

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.

²³¹ Sara Simrall Rorer, American Health Lawyers Association, *Social Media Compliance Challenges: From HIPAA to the NLRA, Social Media and HIPAA Privacy Concerns for Healthcare Providers* <https://www.healthlawyers.org/Events/Programs/Materials/Documents/HHS13/Z_rorer.pdf>.

Clinical photography can be a valuable tool for junior hospital doctors, who are more likely to need frequent diagnostic advice.²³² The use of smartphones for clinical photography is most common in the same cohort.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'.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.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.²³⁶ Unlike stand-alone digital camera, people carry their phones with them, heightening the susceptibility to loss, theft and unauthorised access.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,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,²³⁹ another reported less than 50% used passwords on their phones.²⁴⁰ This is despite the AMA's recommendation that passwords be used on mobile phones containing clinical photographs to prevent unauthorised access.²⁴¹

²³² Jamil, above n 112, 105.

²³³ Nielson, West and Shimizu, above n 20, 2.

²³⁴ *Privacy Act 1988* (Cth) sch 1 pt 4 sub-cl 11.1.

²³⁵ Nielson, West and Shimizu, above n 20, 1; Luo et al, 'Cyberdermatology I: Ethical, Legal, Technologic, and Clinical Aspects of Patient-Physician e-mail' 2009 *27Clinics in Dermatology* 359, 360-1.

²³⁶ Australian Medical Association, above n 79.

²³⁷ Nielson, West and Shimizu, above n 20, 2.

²³⁸ Davis, above n 73, 119.

²³⁹ Kunde, McMeniman and Parker, above n 75, 193.

²⁴⁰ Kirk et al, above n 23, 42.

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.²⁴² When clinical photographs are uploaded to the cloud, disclosure has occurred;²⁴³ if it is an overseas cloud provider, APP 8 governing ‘cross board disclosure’ is invoked.²⁴⁴ 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.²⁴⁵ Failing this, the disclosing entity (the practitioner) can be held accountable, under s 16C of the Privacy Act, for any third party breach²⁴⁶ (e.g. if a practitioner’s cloud provider was hacked).²⁴⁷ Should mandatory data breach reporting become law, the disclosing party would be responsible for reporting an overseas breach.²⁴⁸

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.

²⁴³ ‘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’; Office of the Australian Information Commissioner, Australian Government, *Business Resource: Using and Disclosing Patients’ Health Information* (2015) <<https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-using-and-disclosing-patients-health-information>>.

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,²⁴⁹ 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.).²⁵⁰

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’).

²⁵² *Ibid* sch 1 pt 4 sub-cl 11.1.

²⁵³ Office of the Australian Information Commissioner, *Data Breach Notification Guide: A Guide to Handling Personal Information Security Breaches* <<https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>>.

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.²⁶¹ 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.²⁶² 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.²⁶³

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.²⁶⁴ Accepted by all generations, but especially the younger ones,²⁶⁵ 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.²⁶⁶

According to Statista, an international statistics company, more than two-thirds of US internet users in 2016 were social media users.²⁶⁷ 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.

²⁶⁷ Statista: The Statistics Portal, *Number of Social Media Users Worldwide from 2010 – 2020* <<https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>>.

unique Australian visitors to its site during October 2016²⁶⁸ out of an estimated resident population of 24 million.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.²⁷⁰ There is no reason to believe Australian habits are different.

Professional and personal lives involve ‘boundary-crossing technology’ that is social media.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.²⁷² Despite these boundaries inappropriate posts on social media sites have been made by many medical students.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.²⁷⁴ ‘[U]nidentified’ patient information was posted by medical students unaware their posts gave sufficient detail to violate patient privacy.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.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.²⁷⁷

The AMA’s ‘Clinical Images Guide’²⁷⁸ provides a case study, “*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:

²⁶⁸ Social Media News, *Social Media Statistics Australia - October 2016*

<<http://www.socialmedianews.com.au/social-media-statistics-australia-october-2016/>>.

²⁶⁹ Australian Bureau of Statistic, Australian Government, *Population Clock* (12 November 2016)

<<http://www.abs.gov.au/ausstats/abs%40.nsf/94713ad445ff1425ca25682000192af2/1647509ef7e25faaca2568a900154b63?OpenDocument>>.

²⁷⁰ Statista: The Statistics Portal, above n 267.

²⁷¹ Sánchez Abril, Levin and Del Riego, above n 7, 66.

²⁷² See APP 6 - Use and disclosure: *Privacy Act 1988* (Cth) sch 1 pt 3 sub-cl 6.

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

²⁷⁴ *Ibid* 1309, 1312.

²⁷⁵ *Ibid* 1312, 1314.

²⁷⁶ Simrall, above n 231.

²⁷⁷ *Ibid*.

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.

²⁸¹ Australian Law Reform Commission, above n 148, vol 3, 2223.

²⁸² Carruth and Ginsburg, above n 264, 83.

²⁸³ Australian Medical Association, above n 79.

²⁸⁴ Twenge et al, ‘Egos Inflating Over Time: A Cross-Temporal Meta-Analysis of the Narcissistic Personality Inventory’ 2008 76(4) *Journal of Personality* 875, 899-890.

²⁸⁵ Australian Law Reform Commission, above n 148, vol 3, 2222.

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.²⁸⁶ 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’.²⁸⁷ 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’.²⁸⁸ 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.²⁸⁹

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.²⁹⁰ 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’.²⁹¹

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.

²⁹¹ World Medical Organisation, *WMA Declaration of Geneva* (2016) <<http://www.wma.net/en/30publications/10policies/g1/>>.

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 J²⁹³ 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 1511²⁹⁸ 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

²⁹² Samuel D Warren and Louis D Brandeis, ‘The Right to Privacy’ 1890 4(5) *Harvard Law Review* 193.

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 1838³⁰² 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* <<http://www.medicalboard.gov.au/About.aspx>>.

³⁰⁹ Department of Health Australian Government, *National Registration and Accreditation Scheme (NRSA)* <<http://www.health.gov.au/internet/main/publishing.nsf/Content/work-nras>>.

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 MBA³¹³ 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.³¹⁴

C Confidentiality and Professional Codes

Both patients and society³¹⁵ assume that their doctors will not divulge personal or health information.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.³¹⁷

The right to confidentiality is *not* absolute. It may be forced to yield by legal compulsion; mandatory reporting of certain communicable diseases,³¹⁸ court-sanctioned evidential enquiry³¹⁹ and where law or necessity deems that public

³¹³ *Health Practitioner Regulation National Law (WA) Act 2010* (WA) sch pt 5 s 40; Ian Kerridge, Lowe and McPhee, above n 38, 229.

³¹⁴ Rather, 'the AMA's Code of Ethics sets the standards for ethical behaviour expected of doctors in Australia'; Australian Medical Association, *AMA Code of Ethics – The Foundation of a Doctor-Patient Relationship* <<https://ama.com.au/media/ama-code-ethics-foundation-doctor-patient-relationship>>.

³¹⁵ Richard Cruess and Sylvia Cruess, 'Updating the Hippocratic Oath to Include Medicine's Social Contract' 2014 48 *Medical Education* 95, 96.

³¹⁶ Kim Forrester and Debra Griffiths, *Essentials of Law for Medical Practitioners* (Churchill Livingstone Elsevier Australia, 2011) 65.

³¹⁷ See AHPRA, *Panel Decisions* (2016) <<http://www.ahpra.gov.au/Publications/Panel-Decisions.aspx>>

³¹⁸ Meg Wallace, *Health Care and the Law* (Lawbook Co. Thomson Legal & Regulatory Limited, 3rd ed, 2001) 274 [7.72]; The Royal College of General Practitioners, *Handbook for the Management of Health Information in General Practice* 3rd ed (2014) 12.

³¹⁹ *Brown v Brooks* (Unreported, Supreme Court of New South Wales, McLelland J, 18 August 1988).

interests, such a threat from imminent harm, outweigh respect for individual privacy.
320

Consent, a concept that is inextricably linked to privacy and confidentiality, is also addressed in the MBA code.³²¹ 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.³²² Consent ensures that patient autonomy is respected. Patients retain control over how their information is used or disclosed.³²³ The duty to obtain consent is not only regulated by the MBA code,³²⁴ but is also enshrined in federal privacy law.³²⁵ 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.³²⁶ There exist other 'professional' bodies, such as the RACGP, which support the MBA's Code.³²⁷

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.

³²⁶ RACGP, *Standards for General Practices 4th ed criterion 4.2.1* <<http://www.racgp.org.au/download/documents/Standards/standards4thedition.pdf>>; Medical Board of Australia, above n 26.

³²⁷ Allan and Blake, above n 30, 558; Australian Medical Association, *AMA Code of Ethics – 2004: Editorially Revised 2006* <<https://ama.com.au/position-statement/ama-code-ethics-2004-editorially-revised-2006>>; Medical Board of Australia, above n 26.

D *The Australian Health Practitioner Regulation Agency (AHPRA)*

The Australian health profession is governed by the *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 *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.

³²⁸ Allan and Blake, above n 30, 578.

³²⁹ Ibid 578.

³³⁰ *Health Practitioner Regulation National Law (WA) Act 2010* (WA) sch pt 1 s 3.

³³¹ Allan and Blake, above n 30, 578.

³³² *Health Practitioner Regulation National Law (WA) Act 2010* (WA) s 213(1).

³³³ See Annexure A for full list of National Boards.

³³⁴ AHPRA, *Codes and Guidelines* <<http://www.chiropracticboard.gov.au/Codes-guidelines.aspx>>.

³³⁵ AHPRA, *Social Media Policy* <<http://www.medicalboard.gov.au/Codes-Guidelines-Policies/Social-media-policy.aspx>>.

³³⁶ Ibid.

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.³³⁷ 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.³³⁸ 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.³³⁹ 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').³⁴⁰ The code embodies core values contained within World Medical Association's *Declaration of Geneva* and the

³³⁷ Ibid.

³³⁸ AHPRA panel decisions can be found at: AHPRA, *Panel Decisions* <<http://www.ahpra.gov.au/Publications/Panel-Decisions.aspx>>.

³³⁹ Ibid.

³⁴⁰ Medical Board of Australia, above n 26.

International Code of Medical Ethics.³⁴¹ A serious departure from, or repeated failures to comply with, the Medical Board's code may affect a medical practitioner's medical registration.³⁴² Action may be taken by the MBA that temporarily or permanently restricts or prevents a doctor from practicing medicine within Australia.³⁴³

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 Charter³⁴⁴ a decade later, assuming its current name.³⁴⁵ Membership, which is voluntary, requires post-graduate obligations. Membership benefits include professional pride, formal

³⁴¹ Ibid.

³⁴² Ibid.

³⁴³ *Health Practitioner Regulation National Law (WA) Act 2009* (WA) sch pt 5 ss 39–41.

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/>>.

³⁴⁵ RACGP, *College History: Australian General Practice – A Celebration* <<http://www.racgp.org.au/yourracgp/organisation/history/college-history/australian-general-practice/>>.

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.

³⁴⁸ RACGP, *Development of the RACGP Standards* <RACGP <http://www.racgp.org.au/your-practice/standards/standardsdevelopment/>>.

³⁴⁹ Royal College of General Practitioners, above n 32, 92.

³⁵⁰ RACGP, *Second Draft RACGP Standards for General Practices 5th Edition* (2016) <<http://www.racgp.org.au/download/Documents/Standards/2016/Second-draft-RACGP-Standards-for-general-practices-5th-edition.PDF>>.

added).³⁵¹ The draft 5th edition permits transfer ‘*only after* we receive informed patient *consent*’ (emphasis added).³⁵² Patients’ health records can be ‘accessed...by an appropriate team member’³⁵³ will become accessible by ‘only appropriate team members’.³⁵⁴

3 RACGP Guidelines – What is Missing?

The College’s Standards publication does address information security,³⁵⁵ 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*’³⁵⁶ 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*’.³⁵⁷ 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.³⁵⁸ That said, the publication is predominantly directed at how GPs can leverage social media to promote general practice.³⁵⁹ 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.³⁶⁰ 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').³⁶¹ Interestingly, only one CPD module is consistently required of all doctors, regardless of their specialty status: three-yearly cardiopulmonary resuscitation ('CPR').³⁶² 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.³⁶³ 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.

³⁶⁰ 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/>>.

³⁶¹ Royal College of General Practitioners, above n 32, 80.

³⁶² Ibid.

³⁶³ For example see: Australian Medical Association, *AMA Voted Top Lobby Group by Federal Politicians* (15 August 2006) <<https://ama.com.au/media/ama-voted-top-lobby-group-federal-politicians>>.

The AMA has published its own code of ethics being a ‘body of ethical principles to guide doctors’ conduct’.³⁶⁴ 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’.³⁶⁵

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.³⁶⁶ 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’.³⁶⁷ 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.³⁶⁸

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, APHRA 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.³⁶⁹ 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.

³⁶⁹ AMA represents less 30% of all registered medical practitioners, of whom less than 33% are specialist GPs (VR status): $30\% \times 33\% = 9.9\%$; Medical Board of Australia, *Medical Board of Australia Registrant Data – Reporting Period: October 2015 – December 2015* (2016) AHPRA <<http://www.medicalboard.gov.au/documents/default.aspx?record=WD16%2f19955&dbid=AP&chksum=D6pwdjz7uund3TK21mzsxA%3d%3d>>; AMA, *Australian Medical Association Annual Report 2015* (2016)

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.

<https://ama.com.au/sites/default/files/annual-report/AMA_Annual_Report_2015.pdf>; Paul Smith, *There are some challenges, but in all, general practice is in a healthy space* (28 September 2016) Australian Doctor <<http://www.australiandoctor.com.au/news/news-review/fighting-the-good-gp-fight-1>>.

V FEDERAL PRIVACY LEGISLATION

With Australian privacy legislation for federal, state and territory jurisdictions, application is determined by whether the entity³⁷⁰ is publically or privately owned³⁷¹ 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.³⁷²

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.³⁷³ 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.³⁷⁴

Section 3 of the Privacy Act excludes it affecting the operation of state or territory law,³⁷⁵ 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.

³⁷⁰ As defined by the *Privacy Act 1988* (Cth) s 6 (Entity, Organisation, Corporation referred to collectively in the Act as 'APP entities')

³⁷¹ 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.

³⁷² *Privacy Act 1988* (Cth) s 3.

³⁷³ 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>>.

³⁷⁴ Office of the Australian Information Commissioner, *Business Resource: Handling Health Information under the Privacy Act: A General Overview for Health Service Providers* <<https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-handling-health-information-under-the-privacy-act-a-general-overview-for-health-service-providers>>.

³⁷⁵ *Privacy Act 1988* (Cth) s 3.

³⁷⁶ 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).³⁷⁷

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.’³⁷⁸ Enacted under the Australian Constitution’s ‘express power’ with respect to external affairs,³⁷⁹ 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’.³⁸⁰

The OECD ‘*Guidelines on the Protection of Privacy and Trans-border Flows or Personal Data*’³⁸¹ were designed to facilitate trans-border flow of information between overseas jurisdictions, while ‘protecting privacy and individual liberties’ but furthering ‘economic and social development’.³⁸² 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).

³⁸⁰ International Covenant on Civil and Political Rights, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17 cited in Australian Law Reform Commission, above n 148, vol 1, 104.

³⁸¹ OECD, *Guidelines on the Protection of Privacy and Transborder Flows or Personal Data* <<https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonal data.htm>>.

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.³⁸³ The Privacy Act was amended to cover credit reporting, and then, in 2001, to also regulate the private sector.³⁸⁴

The Privacy Act created the role of Privacy Commissioner, first functioning within the Australian Human Rights Commission,³⁸⁵ 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 2010.³⁸⁶ 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 protection³⁸⁷ revealed concerns that rapid technological advances were eroding personal privacy.³⁸⁸

The report emphasised the need for unified privacy principles³⁸⁹ that covered both public and private entities, the redefinition of terms, such as 'sensitive information',³⁹⁰ the accountability of entities engaging in cross-border data flow,³⁹¹ and the introduction of heavy civil penalties for serious or repetitive privacy breaches.³⁹² In all, the ALRC made 295 recommendations.³⁹³ An 'emerging

³⁸³ Office of the Australian Information Commissioner, Australian Government, *History of the Privacy Act* <<https://www.oaic.gov.au/about-us/who-we-are/history-of-the-privacy-act>>.

³⁸⁴ Ibid.

³⁸⁵ Ibid.

³⁸⁶ Ibid.

³⁸⁷ Australian Law Reform Commission, above n 148, vol 1, 105.

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 privacy³⁹⁴ and the impact of technology and social media was recognised.

Younger people, especially those born between 1980-1994 ('Generation Y')³⁹⁵ appeared willing to make available personal information³⁹⁶ in exchange for the convenience and range of internet services.³⁹⁷ 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.³⁹⁸ This group was also less likely to fully understand how the posting of personal information might adversely affect them.³⁹⁹

Attitudes varied about the need for formal consent prior to online posting of personal information, including photographs,⁴⁰⁰ by a third party. The majority of respondents, however, reported that such information had, in fact, been posted without their knowledge or consent.⁴⁰¹

Fewer 18-24 year olds (50%) than the general adult population (69%) were aware of the existence of Commonwealth privacy laws.⁴⁰² When awareness existed, respondents were often confused by the complexity and application of overlapping state and federal privacy laws.⁴⁰³ 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.⁴⁰⁴ Healthcare providers, key participants in collecting and managing private information, found the federal and state regulations difficult to navigate.⁴⁰⁵

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.

³⁹⁹ Ibid vol 3, 2237-9.

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 Act⁴⁰⁶ incorporated many of the ALRC proposals. A new, unified set of privacy principles, the APPs, applied equally to Commonwealth public agencies and private organisations,⁴⁰⁷ replacing the IPPs and NPPs. Terms were updated or made consistent with other legislation; a ‘record’ now includes ‘electronic or other formats’⁴⁰⁸ and new terms, such as ‘entity’⁴⁰⁹ and ‘APP entity’⁴¹⁰ 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’.⁴¹¹

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’.⁴¹² Biometric information was included in the expanded definition of sensitive information.⁴¹³

The privacy of ‘health information’ was especially important to respondents.⁴¹⁴ ‘Health information’ was expanded to include the ‘physical, mental or psychological health or disability of an individual’.⁴¹⁵

The Amendment Act made provisions for ‘permitted’ exceptions to accommodate circumstances where public interests outweighs 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).

⁴⁰⁷ Australian Law Reform Commission, above n 148, vol 1, 110.

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.

⁴¹¹ Australian Law Reform Commission, above n 148, vol 1, 316.

⁴¹² *Ibid* vol 1, 322 quoting the Biometrics Institute, Biometrics Institute Privacy Code Information Memorandum (2006) 1.

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’⁴¹⁶ is used here, as it is, liberally, through the Privacy Act and the APPs to indicate an objective assessment.⁴¹⁷

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.⁴¹⁸

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.⁴¹⁹

Civil penalty provisions were added for serious or repeated interferences with privacy, as recommended by the ALRC.⁴²⁰ The Commissioner was empowered to apply to the court⁴²¹ for an order against an entity that has allegedly contravened the Privacy Act.⁴²² The maximum penalty a court can order against an individual is \$360,000 and \$1.8 million for entities.⁴²³

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.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.⁴²⁵ Where available OAIC draft guidelines⁴²⁶ have been used to discuss

⁴²⁴ *Privacy Act 1988 (Cth)* sch 1.

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,⁴²⁷ are more rigorous under APP 3.3, than for personal information.⁴²⁸ Collection of the information by governmental agencies must be for either a need that is ‘reasonably necessary’⁴²⁹ 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.⁴³⁰ ‘[R]easonably necessary’ means a legitimate, objective need to justify an interference of privacy when collecting, using or disclosing personal information.⁴³¹

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.⁴³² Unlike agencies, organisations may not collect information unless it is reasonably necessary.

The OAIC’s draft business resource⁴³³ provides examples of collection such as storing patients’ ‘reasonably identifiable’⁴³⁴ photographs, video or audio recordings, identifiable emails containing personal information and collecting and labelling

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/>>.

⁴²⁷ *Privacy Act 1988* (Cth) s 6(1) ‘sensitive information’.

⁴²⁸ *Ibid* sch 1 pt 2 sub-cl 3.1–3.2.

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.

⁴³⁰ *Privacy Act 1988* (Cth) sch 1 pt 2 sub-cl 3.3(a)(i).

⁴³¹ Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 46, 53.

⁴³² *Privacy Act 1988* (Cth) sch 1 pt 2 sub-cl 3.3(a)(ii).

⁴³³ The OAIC is currently finalising ‘Health Privacy Guidance Resources’ following public consultation in 2015; Office of the Australian Information Commissioner, Australian Government, *Business Resource: Collecting Patients’ Health Information* <<https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-collecting-patients-health-information>>.

⁴³⁴ Australian Government, above n 142, 53.

patients' biological samples.⁴³⁵ According to the OAIC guidelines storing clinical photographs in a patient's record⁴³⁶ 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,⁴³⁷ 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.⁴³⁸ Second hand collection would not be a breach if it were 'unreasonable' to collect the information directly.⁴³⁹ 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.⁴⁴⁰

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.⁴⁴¹

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.

⁴³⁸ Ibid sch 1 pt 2 sub-cl 3.6.

⁴³⁹ Ibid sch 1 pt 2 sub-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 sub-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-cl 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.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.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.’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.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.

⁴⁴⁹ *Privacy Act 1988* (Cth) sch 1 pt 3 sub-cl 6.2(a)(i).

⁴⁵⁰ *Ibid* sch 1 pt 3 sub-cl 6.1(a).

⁴⁵¹ Office of the Australian Information Commissioner, above n 243.

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*⁴⁵³ 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’.⁴⁵⁴ 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.⁴⁵⁵ The AMA recommends⁴⁵⁶ 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.⁴⁵⁷

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,⁴⁵⁸ though these types of disclosure are unlikely to occur frequently. Any disclosure required under federal, state or territory law⁴⁵⁹ is permissible under APP 6.2(b). Should an entity ‘reasonably’ believe disclosure is ‘necessary’ for any lawful enforcement related activities⁴⁶⁰ (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.⁴⁶¹ 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

⁴⁵³ [2004] NSWADT 84.

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-cl 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.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 '*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.⁴⁶³ This is in spite of the overseas recipient not being bound by the Australian Privacy Act and its APPs.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.⁴⁶⁵ Additionally, overseas disclosure for a 'permitted general situation'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,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

⁴⁶² See *Privacy Act 1988* (Cth) s 16A(1) item 3.

⁴⁶³ *Privacy Act 1988* (Cth) s 16C (1)-(2), sch 1 pt 3 sub-cl 8.1-8.2.

⁴⁶⁴ *Ibid* s 16C (1)-(2), sch 1 pt 3 sub-cl 8.1-8.2.

⁴⁶⁵ *Ibid* sch 1 pt 3 sub-cl 8.2(a).

⁴⁶⁶ *Ibid* s 16A(1) item 1-3, 6-7.

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.

⁴⁷⁵ Office of the Australian Information Commissioner, Australian Government, *Guide to Securing Personal Information* (2015) <<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>>.

as storage and back up.⁴⁷⁶ 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.⁴⁷⁷ 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,⁴⁷⁸ 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.⁴⁷⁹ Consequently, a breach of an APP is deemed an ‘interference with the privacy of an individual’.⁴⁸⁰

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.⁴⁸¹ The Privacy Act empowers the Privacy Commissioner to conduct discretionary assessments,⁴⁸² to investigate matters where complaints have been made,⁴⁸³ or to commence a ‘Commissioner Initiated Investigation’⁴⁸⁴ where conduct indicates possible APP non-compliance. The Commissioner may then make an enforceable determination⁴⁸⁵ outlining the requirements to rectify the breach and preventative action needed to avoid future breaches.⁴⁸⁶ The determination may include a compensatory payment for loss or damage,⁴⁸⁷ which is not confined to financial loss and can be awarded for emotion distress.⁴⁸⁸ Alternatively, the Commissioner may prefer to seek a court order.⁴⁸⁹

Serious or repeated privacy breaches are addressed by s 13G, a ‘civil penalty provision’,⁴⁹⁰ which can attract a civil penalty of up to \$360,000 for individuals and \$1.8 million for entities.⁴⁹¹ Although dealt with in a single section,⁴⁹² serious and repeated interferences are separate concepts,⁴⁹³ and the civil penalty can only be made by court order, following the Commissioner application.⁴⁹⁴ The affected party may also seek a compensatory order for loss or damage, both pecuniary, and non-

⁴⁷⁹ Ibid ss 6A(2)–(5), 13B–D.

⁴⁸⁰ Ibid (Cth) s 13(1)(a).

⁴⁸¹ The Office of the Information Commissioner, Australian Government, *Chapter 6: Civil Penalties – Serious or Repeat Interferences with Privacy and other Penalty Provisions* <<https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties>>.

⁴⁸² *Privacy Act 1988* (Cth) s 33C.

⁴⁸³ Ibid s 40(1).

⁴⁸⁴ Ibid s 40(2).

⁴⁸⁵ Ibid s 55A.

⁴⁸⁶ Ibid s 52(1)(b)(ia).

⁴⁸⁷ Ibid s 52(1)(b)(iii).

⁴⁸⁸ Ibid s 52(1AB); Explanatory Memorandum, Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Cth) 245.

⁴⁸⁹ *Privacy Act 1988* (Cth) s 80W.

⁴⁹⁰ See *Privacy Act 1988* (Cth) s 80U regarding the Act’s sections or subsections that are penalty provisions.

⁴⁹¹ Above n 423.

⁴⁹² *Privacy Act 1988* (Cth) s 13G.

⁴⁹³ The Office of the Information Commissioner, Australian Government, above n 481.

⁴⁹⁴ 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.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,⁵⁰⁷ and affected individuals are not compensated by this order.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.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.⁵¹⁰ This incident is believed to be Australia's largest data breach incident to date.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.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?’⁵¹³

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

⁵⁰⁶ The Office of the Information Commissioner, above n 481.

⁵⁰⁷ *Privacy Act 1988* (Cth) s 80X; Note: Compensation orders under sections 25, 25A only apply to credit reporting.

⁵⁰⁸ *Privacy Act 1988* (Cth) s 80W; The Office of the Information Commissioner, above n 481.

⁵⁰⁹ *IV' and 'IW'* [2016] AICmr 41 (27 June 2016).

⁵¹⁰ Australian Red Cross Blood Service, *Blood Service Apologies for Donor Data Leak* (28 October 2016) <<http://www.donateblood.com.au/media/news/blood-service-apologises-donor-data-leak>>.

⁵¹¹ Troy Hunt, ‘The Red Cross Blood Service: Australia's largest ever leak of personal data’ on TroyHunt.com (28 October 2016) <<https://www.troyhunt.com/the-red-cross-blood-service-australias-largest-ever-leak-of-personal-data/>>.

⁵¹² Australian Red Cross Blood Service, above n 510.

⁵¹³ Jim Birch and Shelly Park, *A Note From the Blood Service Chief Executive and the Chair* <<http://info.donateblood.com.au/>>; Shelly Park, *Update from Shelly Park, Chief Executive* (29 October 2016) <<http://info.donateblood.com.au/>>.

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.

⁵¹⁶ Office of the Australian Information Commissioner, Australian Government, *Comment by the Australian Privacy Commissioner – Australian Red Cross* (28 October 2016) <<https://www.oaic.gov.au/media-and-speeches/statements/comment-by-the-australian-privacy-commissioner-australian-red-cross>>.

⁵¹⁷ Office of the Australian Information Commissioner, Australian Government, *K- Mart Australia Data Breach* (1 Oct 2015) <<https://www.oaic.gov.au/media-and-speeches/statements/kmart-australia-data-breach>>; Office of the Australian Information Commissioner, Australian Government, *David Jones Data Breach* (2 Oct 2015) <<https://www.oaic.gov.au/media-and-speeches/statements/david-jones-data-breach>>.

⁵¹⁸ Office of the Australian Information Commissioner, Australian Government, *Data Breach: AussieTravelCover* (2 June 2015) <<https://www.oaic.gov.au/media-and-speeches/statements/data-breach-aussietravelcover>>.

⁵¹⁹ *Ibid*.

⁵²⁰ Will Ockenden and Benjamin Svein, *Aussie Travel Cover has Hundreds of Thousands of Records Stolen in Hacking, Policy Holders Not Informed* (19 Jan 2015) ABC News <<http://www.abc.net.au/news/2015-01-19/aussie-travel-cover-hacked-customers-not-told/6025652>>.

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?⁵²² 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’⁵²³ 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.⁵²⁴

The above-mentioned breaches have compromised personal information entrusted to entities, highlighting the importance of establishing and implementing sufficient security measures.⁵²⁵ 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.

⁵²³ Alastair MacGibbons 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 <<http://www.canberra.edu.au/cis/storage/Australian%20Attitudes%20Towards%20Privacy%20Online.pdf>>.

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,⁵²⁶ 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.⁵²⁷ The HITECH Act supports and extends the ‘*Health Insurance Portability and Accountability Act 1996*’ (US) (‘HIPAA’),⁵²⁸ which lays out health information privacy, security and enforcement requirements.⁵²⁹ To this was added the HIPAA ‘Final Rule’ (also referred to as the ‘Omnibus Rule’) coming into force in September 2013.⁵³⁰ 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.⁵³¹ 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.⁵³² 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.⁵³³ 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.

⁵²⁷ 42 USC § 17932 (2009).

⁵²⁸ 42 USC § 1320d-5 (2009); Laurie A Rinehart-Thompson, Beth M Hjort and Bonnie S Cassidy, ‘Redefining the Health Information Management Privacy and Security Role’ 2009 6 *Perspectives in Health Information Management* 1–3.

⁵²⁹ 42 USC § 1320d.

⁵³⁰ 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, 5566, 5568–9.

⁵³¹ *Ibid.*

⁵³² Rinehart-Thompson, Hjort and Cassidy, above n 528, 1–3.

⁵³³ Department of Health and Human Services, *Data Breach Results in \$4.8 million HIPAA Settlement* (7 May 2014) <<http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html>>.

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.

⁵³⁴ Department of Health and Human Services, *\$4.8 million HIPAA Settlement Underscores Importance of Managing Security Risks* (18 October 2016) <<http://www.hhs.gov/about/news/2016/10/18/214-million-hipaa-settlement-underscores-importance-managing-security-risk.html>>.

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,⁵³⁵ 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.⁵³⁶ Social media is part of daily life for many young adults⁵³⁷ and has permeated the professional workplace, not being confined to the personal sphere.⁵³⁸ 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,⁵³⁹ which is largely hospital-based, before they can acquire general registration;⁵⁴⁰ this may provide the opportune educational structure for incorporation of a digital media module.⁵⁴¹ Content should include doctors' legal and professional privacy

⁵³⁵ Kornhaber, Betihavas and Baber, above n 6, 301.

⁵³⁶ Swick et al, 'Teaching Professionalism in Undergraduate Medical Education' 1999 282(9) *Journal of American Medical Association* 830, 830.

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%5bv2%5d&dbid=AP&hksun=PvYzX0nEOt%2bYT0wNVghlKA%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.⁵⁴² 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’.⁵⁴³ 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)⁵⁴⁴ 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’.⁵⁴⁵ The revalidation components would compose of ‘strengthened CPD’ programs, and identifying and supporting poorly performing doctors,⁵⁴⁶ with a focus on keeping doctors’

⁵⁴² Chretien et al. suggested a similar approach, though it was posed 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.

⁵⁴⁵ Medical Board of Australia, *Options for Revalidation in Australia – Discussion Paper* (August 2016) <<http://www.medicalboard.gov.au/documents/default.aspx?record=WD16%2F21163&dbid=AP&chksum=1AmBXmPS80XN5gNGp%2BQvlQ%3D%3D>>.

⁵⁴⁶ Ibid.

knowledge up-to-date.⁵⁴⁷ If implemented, CPD training will aim to be ‘more effective, flexible and dynamic’.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 *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.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.

⁵⁴⁷ Medical Board of Australia, *Medical Board Consults on Revalidation in Australia* (16 August 2016) <<http://www.medicalboard.gov.au/News/2016-08-16-revalidation.aspx>>.

⁵⁴⁸ Medical Board of Australia, above n 545.

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

VIII GLOSSARY OF TERMS

<i>Accountability Approach</i>	APP Entity who makes a disclosure to an overseas recipient, will be held accountable for the recipient's APP breach in some circumstances; <i>Privacy Act</i> section 16C, APP 8
<i>Agency</i>	Refer to section 6(1) of the <i>Privacy Act</i>
<i>APP Entity</i>	An 'agency' or 'organisation' as defined in section 6(1) – 'Entity' of the <i>Privacy Act</i>
<i>Australian Privacy Principles</i>	Schedule 1 of the <i>Privacy Act</i>
<i>APP Breach</i>	Refer to section 6A of the <i>Privacy Act</i>
<i>Civil Penalty Order</i>	Refer to section 80W(4) of the <i>Privacy Act</i>
<i>Civil Penalty Provision</i>	Refer to section 80U of the <i>Privacy Act</i>
<i>Clinical Photography</i>	A photograph taken for medical purposes (also referred to as digital photography or clinical image)
<i>Cloud Storage</i>	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
<i>Code / MBA Code</i>	The Medical Board of Australia's Professional Code of Conduct: Good Medical Practice
<i>Collects</i>	An entity collects personal information only if the entity records that information in a record; <i>Privacy Act</i> s 6(1)

<i>Consent</i>	Permission given by someone to do something to his or her person. Consent can be either express or implied
<i>De-identified information</i>	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 <i>Privacy Act</i>
<i>Dermatologist</i>	A medical practitioner that specialises in skin
<i>Entity</i>	An agency, organisation or small business operator
<i>Health Information</i>	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 <i>Privacy Act</i>
<i>Health Service</i>	Refer to section 6FB of the <i>Privacy Act</i>
<i>Health Service Provider</i>	A provider of health services, or holder of <i>health information</i> , even if providing health services is not the organisation’s primary function or activity
<i>General Practitioner (GP)</i>	A medical practitioner/doctor who specialises in general practice
<i>Interference (of privacy)</i>	Refer to section 13–13F of the <i>Privacy Act</i>
<i>Lesion</i>	An irregular region of external body tissue affected by disease
<i>Permitted General Situation</i>	Refer to section 16A of the <i>Privacy Act</i>
<i>Permitted Health Situation</i>	Refer to section 16B of the <i>Privacy Act</i>

<i>Personal information</i>	Information, whether fact or opinion, about a specific individual who is identified or reasonably identifiable; defined by s 6(1) of the <i>Privacy Act</i>
<i>Organisation</i>	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 <i>Privacy Act</i>
<i>Practitioner</i>	A licensed medical practitioner (a doctor)
<i>Primary Purpose</i>	The main reason behind the action for collection, use or disclosure
<i>Private Entity</i>	Any organisation not owned by the Australia Government
<i>Public Entity</i>	Any Australian Government Agency Australian
<i>Reasonableness</i>	The appropriateness of decision-making that reflects an objective standard having regard to the circumstances and context (see <i>LexisNexis Concise Australian Legal Dictionary, 4th ed</i>)
<i>Record</i>	A document, electronic device or other device as defined in s 6(1) of the <i>Privacy Act</i>
<i>Registrar</i>	A registered medical practitioner who has is undertaking specialty accredited training (e.g. a doctor who is training in dermatology)
<i>Responsible Person</i>	Refer to section 6AA of the <i>Privacy Act</i>
<i>Secondary Purpose</i>	Any purpose that is not the primary purpose

<i>Store and forward</i>	A process where the original party records information, for example, a photograph, then electronically transmits a copy to another party
<i>Sensitive Information</i>	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
<i>Small Business Operator</i>	Refer to section 6D of the <i>Privacy Act</i>

IX ACRONYMS

ACT	Australian Capital Territory
ACGP	Australian College of General Practitioners
AHPRA	Australian Health Practitioner Regulation Agency
ALRC	Australian Law Reform Commission
AMA	Australian Medical Association
APPs	Australian Privacy Principles
ATC	Aussie Travel Cover
AUS	Australia
CPD	Continuing Professional Development
CPR	Cardiopulmonary resuscitation
ED	Emergency Department
EMR	Electronic Medical Record
GMC	General Medical Council (UK)
GP	General Practitioner
HHS	Health and Human Services, US Department of
HIPAA	Health Insurance Portability and Accountability Act 1996
HITECH	Health Information Technology and Economic Clinical Health Act
IPPs	Information Privacy Principles
MBA	Medical Board of Australia
MIIAA	Medical Indemnity Industry Association of Australia
NPPs	National Privacy Principles
NRAS	National Registration and Accreditation Scheme
NSW	New South Wales
NT	Northern Territory
OAIC	Office of the Australian Information Commissioner

OCR	Office of Civil Rights (US)
OECD	Organisation for Economic Cooperation and Development
QLD	Queensland
RACD	Royal Australian College of Dermatologists
RACGP	Royal Australian College of General Practitioners
RACS	Royal Australian College of Surgery
RCGP	Royal College of General Practitioners (UK)
SA	South Australia
TAS	Tasmania
UK	United Kingdom
UCSF-MC	University of California, San Francisco Medical Centre
US	United States
VIC	Victoria
VR	Vocational Registration
WA	Western Australia
WMA	World Medical Association

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)

Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008)

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, 'The Ethical Context of Clinical Photography' 2002 25(3) *Journal of Audiovisual Media in Medicine* 106

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

Berle, Ian, 'Privacy and Confidentiality: What is the Difference?' 2011 34(1) *Journal of Visual Communication* 43

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

Butt, Peter and David Hamer (eds), *LexisNexis Concise Australian Legal Dictionary* (LexisNexis Butterworths, 4th ed, 2011)

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

Comfere, Nneka I, Olayemi Sokumbi, Victor M Montori, Annie LeBlanc, Larry J Prokop, Hassan Murad and Jon C Tilburt, 'Provider-to-Provider Communications in Dermatology and Implications of Missing Clinical Information in Skin Biopsy Requisition Forms: A Systematic Review' 2014 53 *International Journal of Dermatology* 549

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

Cunniff, Christopher, Janice Byrne, Louanne Hudgins, John Moeschler, Ann Haskins Olney, Richard Pauli, Lauri Seaver, Cathy Stevens and Christopher Figone, 'Informed Consent for Medical Photographs' 2000 2(6) *Genetics in Medicine* 353

Davis, Michael, 'Safeguarding Patient Privacy in the Context of Clinical Innovation' 2014 1 *Australian Health Law Bulletin* 117

De Roubaix, J A M, 'Beneficence, Non-Maleficence, Distributive Justice and Respect for Patient Autonomy – Reconcilable Ends in Aesthetic Surgery?' 2011 64 *Journal of Plastic, Reconstructive & Aesthetic Surgery* 11

Dean, Richard, *The Value of Humanity in Kant's Moral Theory* (Oxford University Press, 2006)

Forrester, Kim and Debra Griffiths, *Essentials of Law for Medical Practitioners* (Churchill Livingstone Elsevier Australia, 2011)

Franchitto, Nicolas, Laurent Gavarri, Fabrice Dédouit, Norbet Telmon and Daniel Rougé, 'Photographs, Patient Consent and Scientific Publications: Medicolegal aspects in France' 2008 15 *Journal of Forensic and Legal Medicine* 210

Guffin, Peter, 'Data Security Breach Notification Requirements in the United States: What You Need to Know' 2011 4 *The Quarterly Journal of PRISM International* 6

Harting, M, J DeWees, K Vela and R Khirallah, 'Medical Photography: Current Technology, Evolving Issues and Legal Perspectives' 2015 69 *International Journal of Clinical Practice* 401

Higgins, Gerald, 'The History of Confidentiality in Medicine' 1989 (35) *Canadian Family Physician* 921

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

Hood, Catherine, Tony Hope and Phillip Dove, 'Videos, Photographs and Patient Consent' 1998 316 *British Medical Journal* 1009

Hubbard, V, D Goodard and S Walker, 'An Online Survey of the Use of Digital cameras by Members of the British Association of Dermatologists' 2009 34 *Clinical and Experimental Dermatology* 492

Jamil, F, 'Smartphone Photography Oral and Maxillofacial Surgery' 2016 54 *British journal of Oral and Maxillofacial Surgery* 104

Jin, Ming, Leonard Goldberg, Paul Friedman and Arash Kimyai-Asadi, 'Surgical Pearl: The use of Polaroid Photography for Mapping Mohs Surgery Sections' 2005 52 *Journal of American Academy of Dermatology* 511

Johns, Martin, 'Informed Consent for Clinical Photographs' 2002 25(2) *Journal of Audiovisual Media in Medicine* 59

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

Kornhaber, Rachel, Vasilki Betihavas and Rodney Baber, 'Ethical Implications of Digital Images for Teaching and Learning Purpose: An Integrative Review' 2015 8 *Journal of Multidisciplinary Healthcare* 299

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

Lakdawala, Nikita, Lionel Bercovitch and Jane Grant-Kels, 'Picture is Worth a Thousand Words: Ethical Dilemmas Presented by Storing Digital Photographs in Electronic Health Records' 2013 69 *Journal of American Academy of Dermatology* 473

Lasagna, Louis, 'Modern Hippocratic Oath' 1995 72(11) *Medical Economics* 202

Lau, Catherine, Hagan Schumacher and Michael Irwin, 'Patients' Perception of Medical Photography' 2010 63 *Journal of Plastic, Reconstructive & Aesthetic Surgery* e507

Lenardis, Matthew, Robert Solomon and Fok-Han Leung, 'Store and Forward Tele dermatology: A case Report' 2014 7 *BMC Research Notes* 588

Lockwood, Gillian, 'Confidentiality' 2007 3(3) *The Foundation Years* 107

Luo, John, Christopher Logan, Thomas Long and Lionel Bercovitch, 'Cyberdermatology I: Ethical, Legal, Technologic, and Clinical Aspects of Patient-Physician e-mail' 2009 27*Clinics in Dermatology* 359

Mahar, Patrick, Peter Foley, Alexander Sheed-Finck and Christopher Baker, 'Legal Considerations of Consent and Privacy in the Context of Clinical Photography in Australian Medical Practice' 2013 198(1) *Medical Journal of Australia* 48

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

Napoli, Lisa, 'The Doctrine of Informed Consent and Women: The Achievement of Equal Value and Equal Exercise of Autonomy' 1996 4 *Journal of Gender & the Law* 335

Nielson, Colton, Cameron West and Ikue Shimizu, 'Review of Digital Image Security in Dermatology' 2015 21(10) *Dermatology Online Journal* 1

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

Payne, Karl, Arpan Tahim, Alexander McGoodson, Margaret Delaney and Kathleen Fan, 'A Review of Current Clinical Photography Guidelines in Relation to Smartphones Publishing of Medical Images' 2012 35(4) *Journal of Visual Communication in Medicine* 188

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

Risser, Jessica, Zakiya Pressley, Emir Veledar, Carl Washington and Suephy Chen, 'The Impact of Total Body Photography on Biopsy Rate in Patients from a Pigmented Lesion Clinic' 2007 57(3) *Journal of American Academy of Dermatology* 428

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

Sánchez Abril, Patricia, Avner Levin and Alissa Del Riego, 'Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee' 2012 49(1) *American Business Law Journal* 63

Scheinfeld, Noah, Kelly Flanigan, Mark Moshiyakhov and Jeffrey Weinberg, 'Trends in the Use of Cameras and Computer Technology Among Dermatologists in New York City 2001 – 2002' 2003 29(8) *Dermatologic Surgery* 822

Scheinfeld, Noah and Brooke Rothstein, 'HIPAA, Dermatology Images, and the Law' 2013 32 *Seminars in Cutaneous Medicine and Surgery* 199

Schwab, Abraham, Lily Frank and Nada Gligorov, 'Saying Privacy, Meaning Confidentiality' 2011 11(11) *The American Journal of Bioethics* 44

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

Segal, Jeffrey and Michael Sacopulos, 'Photography Consent and Related Legal Issues' 2010 18 *Facial Plastic Surgery Clinic North America* 237

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

Stauch, Marc, Kay Wheat and John Tingle, *Text, Cases & Material on Medical Law* (Routledge Cavendish, 5th ed, 2006)

Stevenson, Paul, Anna Finnane and Peter Soyer, 'Teledermatology and Clinical Photography: Safeguarding Patient Privacy and Mitigating Medico-legal Risk' 2016 204(5) *Medical Journal of Australia* 198

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

Taylor, D McG, E Foster, C S J Dunkin and A M Fitzgerald, 'A Study of the Personal Use of Photography within Plastic Surgery' 2008 61 *Journal of Plastic, Reconstructive & Aesthetic Surgery* 37

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

Wallace, Meg, *Health Care and the Law* (Lawbook Co. Thomson Legal & Regulatory Limited, 3rd ed, 2001)

Warren, Samuel D and Louis D Brandeis, 'The Right to Privacy' 1890 4(5) *Harvard Law Review* 193

Warshaw, Erin M, Yonatan J Hillman, Nancy L Greer, Emily M Hagel, Roderick MacDonalson, Indulis R Rutks and Timothy J Wilt, 'Teledermatology for Diagnosis and Management of Skin Conditions: A systematic Review' 2011 64(4) *Journal of American Academy of Dermatology* 759

White, Ben, Fiona McDonald and Lindy Willmott, *Health Law in Australia* (Thomson Reuters (Professional) Australia Limited, 2nd ed, 2014)

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] AICmr 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

Schloendorff 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 Information Technology for Economic and Clinical Health Act, Pub L No 111-5, § 13402, 123 Stat 260 (2009) (US)

Health Insurance Portability and Accountability Act of 1996, Pub L No 104-191, § 1171, 110 Stat 2120 (2010) (US)

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*

International Covenant on Civil and Political Rights, Australia, opened for signature 16 December 1966, [1980] ATS 23 (entered into force 23 March 1976)

E *Other*

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

AHPRA, *Codes and Guidelines* < <http://www.medicalboard.gov.au/Codes-Guidelines-Policies.aspx> >

AHPRA, *Panel Decisions* (2016) <<http://www.ahpra.gov.au/Publications/Panel-Decisions.aspx>>

AHPRA, *Possible Outcomes* (2016) <<http://www.ahpra.gov.au/Notifications/Find-out-about-the-complaints-process/Possible-outcomes.aspx>>

AHPRA, *Social Media Policy* < <http://www.medicalboard.gov.au/Codes-Guidelines-Policies/Social-media-policy.aspx>>

Alder, Steve and Andrew Kelleher, HIPAA Journal, *HIPAA Compliance Guide*
<<http://www.hipaajournal.com/hipaa-compliance-guide/>>

Australian Bureau of Statistic, Australian Government, *Population Clock* (12 November 2016)
<<http://www.abs.gov.au/ausstats/abs%40.nsf/94713ad445ff1425ca25682000192af2/1647509ef7e25faaca2568a900154b63?OpenDocument>>

Australian Government, *Australian Privacy Principles Companion Guide*
<http://www.aph.gov.au/~/_media/wopapub/senate/committee/fapa_ctte/completed_inquires/2010-13/priv_exp_drafts/guide/companion_guide.ashx>

Australian Medical Association, *AMA Code of Ethics – 2004. Editorially Revised 2006* <<https://ama.com.au/position-statement/ama-code-ethics-2004-editorially-revised-2006>>

Australian Medical Association, *AMA Code of Ethics – The Foundation of a Doctor-Patient Relationship* <<https://ama.com.au/media/ama-code-ethics-foundation-doctor-patient-relationship>>

Australian Medical Association, *AMA Voted Top Lobby Group by Federal Politicians* (15 August 2006) <<https://ama.com.au/media/ama-voted-top-lobby-group-federal-politicians>>

Australian Medical Association, *Australian Medical Association Annual Report 2015* (2016) <https://ama.com.au/sites/default/files/annual-report/AMA_Annual_Report_2015.pdf>

Australian Medical Association, *Clinical Images and the use of Personal Mobile Devices*
<https://ama.com.au/sites/default/files/FINAL_AMA_Clinical_Images_Guide_0.pdf>

Australian Medical Association, *Privacy and Health Record Resource Handbook: For Medical Practitioners in the Private Sector* (2014)

Australian Medical Association, *Use and Disclosure of Clinical Images*
<<https://ama.com.au/use-and-disclosure-clinical-images>>

Australian Red Cross Blood Service, *Blood Service Apologies for Donor Data Leak*
(28 October 2016) <<http://www.donateblood.com.au/media/news/blood-service-apologises-donor-data-leak>>

Barbaro, Michael and Tom Zellar, *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>

Birch, Jim and Shelly Park, *A Note From the Blood Service Chief Executive and the Chair* <<http://info.donateblood.com.au/>>

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>>

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
<<http://www.mbsonline.gov.au/internet/mbsonline/publishing.nsf/Content/Downloads-201607>>

Department of Health, Australian Government, *National Registration and Accreditation Scheme (NRSA)*
<<http://www.health.gov.au/internet/main/publishing.nsf/Content/work-nras>>

Department of Health and Human Services, *Data Breach Results in \$4.8 million HIPAA Settlement* (7 May 2014) <<http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html>>

Department of Health and Human Services, *\$4.8 million HIPAA Settlement Underscores Importance of Managing Security Risks* (18 October 2016) <<http://www.hhs.gov/about/news/2016/10/18/214-million-hipaa-settlement-underscores-importance-managing-security-risk.html>>

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

Fagan, Xaiver, *An Annual Update for MDA National Ophthalmology Members: Imaging in Ophthalmology and How it Affects You* <<http://www.mdanational.com.au/~media/Files/MDAN-Corp/Publications/Ophthalmology-Update-2015.pdf?la=en>>

Gane, Victor, *Patient interaction and HIPAA compliance in our Digital World* (7 May 2014) *Prime: International Journal of Aesthetic and Anti-Ageing Medicine* <<https://www.prime-journal.com/patient-interaction-and-hipaa-compliance-in-our-digital-world/>>

Hunt, Troy, 'The Red Cross Blood Service: Australia's Largest Ever Leak of Personal Data' on TroyHunt.com (28 October 2016) <<https://www.troyhunt.com/the-red-cross-blood-service-australias-largest-ever-leak-of-personal-data/>>

Identity Theft Centre, *Identity Theft Resource Centre Breach Report Hits Near Record High in 2015* <<http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html>>

International Committee of Medical Journal Editors, *Protection of Research Participants* <<http://www.icmje.org/recommendations/browse/roles-and-responsibilities/protection-of-research-participants.html>>

Krashinsky, Susan, *Google Broke Canada's Privacy Laws with Targeted Health Ads, Watchdog Says* (15 January 2014) *The Globe and Mail* <<http://license.icopyright.net/user/viewFreeUse.act?fuid=MjM5MjExODg%3D>>

Liew, Ruth 'Top Australian Cyber Crime Targets for 2016 Named' *Australian Financial Review* (Online), 24 November 2015 <<http://www.afr.com/technology/top-australian-cyber-crime-targets-for-2016-named-20151120-gl40zk>>

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

<<http://www.canberra.edu.au/cis/storage/Australian%20Attitudes%20Towards%20Privacy%20Online.pdf>>

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

<<https://www.mja.com.au/careers/198/3/online-security>>

MDA National, '*MDA National*' <<http://www.mdanational.com.au/>>

MDA National, *Medical Records*

<<http://www.mdanational.com.au/~media/Files/MDAN-Corp/Medico-Legal/Medical-Records.pdf?la=en>>

Medical Board of Australia, *About* <<http://www.medicalboard.gov.au/About.aspx>>

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*

(16 August 2016) <<http://www.medicalboard.gov.au/News/2016-08-16-revalidation.aspx>>

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

<<http://www.medicalboard.gov.au/documents/default.aspx?record=WD16%2f19955&dbid=AP&chksum=D6pwdjz7uund3TK21mzsxA%3d%3d>>

Medical Board of Australia, *Options for Revalidation in Australia – Discussion Paper* (August 2016) < Medical Board of Australia, *Options for Revalidation in Australia – Discussion Paper* (August 2016)

<<http://www.medicalboard.gov.au/documents/default.aspx?record=WD16%2F21163&dbid=AP&chksum=1AmBXmPS80XN5gNGp%2BQvIQ%3D%3D>>

Melbourne Pathology, *Online Results* (2016)

<[http://www.mps.com.au/doctors/online-results-\(fetch,-webster\).aspx](http://www.mps.com.au/doctors/online-results-(fetch,-webster).aspx)>

MIA Radiology, *MIA Direct* (2015)

<<http://www.miaradiology.com.au/Referrers/MIA-Direct>>

MoleScope, *Products* <<https://molescope.com/product/>>

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>

New London Consulting, *Australia: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* (28 February 2012) Fair Warning

<[http://www.fairwarning.com/wp-content/uploads/2015/09/2012-04-WP-](http://www.fairwarning.com/wp-content/uploads/2015/09/2012-04-WP-AUSTRALIA-PATIENT-SURVEY1.pdf?utm_source=survey&utm_medium=www.fairwarning.com&utm_term=australia+patient+privacy+survey&utm_content=australia+patient+privacy+survey&utm_campaign=website+content)

AUSTRALIA-PATIENT-

SURVEY1.pdf?utm_source=survey&utm_medium=www.fairwarning.com&utm_term=australia+patient+privacy+survey&utm_content=australia+patient+privacy+survey&utm_campaign=website+content>

Ockenden, Will and Benjamin Sveen, *Aussie Travel Cover has Hundreds of*

Thousands of Records Stolen in Hacking, Policy Holders Not Informed (19 Jan 2015)

ABC News <<http://www.abc.net.au/news/2015-01-19/aussie-travel-cover-hacked-customers-not-told/6025652>>

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,

Advisory Guidelines <<https://www.oaic.gov.au/agencies-and-organisations/advisory-guidelines/>>

Office of the Australian Information Commissioner, Australian Government,

Assessments <<https://www.oaic.gov.au/privacy-law/assessments/>>

Office of the Australian Information Commissioner, Australian Government, *Australian Information Commissioner Act* <<https://www.oaic.gov.au/about-us/who-we-are/australian-information-commissioner-act>>

Office of the Australian Information Commissioner, Australian Government, *Business Resource: Collecting Patients' Health Information* (2015) <<https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-collecting-patients-health-information>>

Office of the Australian Information Commissioner, Australian Government, *Business Resource: Handling Health Information under the Privacy Act: A General Overview for Health Service Providers* (2015) <<https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-handling-health-information-under-the-privacy-act-a-general-overview-for-health-service-providers>>

Office of the Australian Information Commissioner, Australian Government, *Business Resource: Using and Disclosing Patients' Health Information* (2015) <<https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-using-and-disclosing-patients-health-information>>

Office of the Information Commissioner, Australian Government, *Chapter 6: Civil Penalties – Serious or Repeat Interferences with Privacy and other Penalty Provisions* <<https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties>>

Office of the Australian Information Commissioner, Australian Government, *Comment by the Australian Privacy Commissioner – Australian Red Cross* (28 October 2016) <<https://www.oaic.gov.au/media-and-speeches/statements/comment-by-the-australian-privacy-commissioner-australian-red-cross>>

Office of the Australian Information Commissioner, Australian Government, *Data Breach: AussieTravelCover* (2 June 2015) <<https://www.oaic.gov.au/media-and-speeches/statements/data-breach-aussietravelcover>>

Office of the Australian Information Commissioner, Australian Government, *Data Breach Notification Guide: A Guide to Handling Personal Information Security Breaches* (2015) <<https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>>

Office of the Australian Information Commissioner, Australian Government, *General Practice Clinics - APP 1 Privacy Policy Assessment* (April 2016) <<https://www.oaic.gov.au/privacy-law/assessments/general-practice-clinics-app-1-privacy-policy-assessment>>

Office of the Australian Information Commissioner, Australian Government, *Guide to Securing Personal Information* (2015) <<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>>

Office of the Australian Information Commissioner, Australian Government, *History of the Privacy Act* <<https://www.oaic.gov.au/about-us/who-we-are/history-of-the-privacy-act>>

Office of the Australian Information Commissioner, Australian Government, *K-Mart Australia Data Breach* (1 Oct 2015) <<https://www.oaic.gov.au/media-and-speeches/statements/kmart-australia-data-breach>>

Office of the Australian Information Commissioner, Australian Government, *Other Privacy Jurisdictions* <<https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions>>

Office of the Australian Information Commissioner, Australian Government, *Privacy Business Resource 4: De-identification of Data and Information* (2015) <<https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information>>

Office of the Australian Information Commissioner, Australian Government, *What Should Health Service Providers Consider Before Taking a Photo of a Patient on a Mobile Phone?* <<https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/health-service-providers/what-should-health-service-providers-consider-before-taking-a-photo-of-a-patient-on-a-mobile-phone>>

Park, Shelly, *Update from Shelly Park, Chief Executive* (29 October 2016) <<http://info.donateblood.com.au/>>

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

<<http://dermcast.tv/pharmacology-and-therapeutics-panel-discussion-colby-evans-md-jeffrey-callen-md-and-whitney-high-md/>>

Pillay, Samantha, *Mandatory Data Breach Notification – What does it mean for Healthcare Providers?* (21 September 2016) Lexology Associate Corporate Counsel Australia <[http://www.lexology.com/library/detail.aspx?g=5d0acc25-35e2-462c-bb31-](http://www.lexology.com/library/detail.aspx?g=5d0acc25-35e2-462c-bb31-f78495b23972&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Australian+IHL+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2016-10-04&utm_term=>)

[f78495b23972&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-](http://www.lexology.com/library/detail.aspx?g=5d0acc25-35e2-462c-bb31-f78495b23972&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Australian+IHL+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2016-10-04&utm_term=>)

[+General+section&utm_campaign=Australian+IHL+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2016-10-04&utm_term=>](http://www.lexology.com/library/detail.aspx?g=5d0acc25-35e2-462c-bb31-f78495b23972&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Australian+IHL+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2016-10-04&utm_term=>)

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/>>

RACGP, *College History: The RACGP Medical Record System: A Short Account of the Development of the Record*

<<http://www.racgp.org.au/yourracgp/organisation/history/college-history/racgp-medical-record-system/>>

RACGP, *College History: Australian General Practice – A Celebration*

<<http://www.racgp.org.au/yourracgp/organisation/history/college-history/australian-general-practice/>>

RACGP, *Development of the RACGP Standards* <RACGP

<http://www.racgp.org.au/your-practice/standards/standardsdevelopment/>>

RACGP, *QI&CPD 2014-16 Program* <<https://www.racgp.org.au/education/qicpd-program/>>

RACGP, *Second Draft RACGP Standards for General Practices 5th Edition* (2016)

<<http://www.racgp.org.au/download/Documents/Standards/2016/Second-draft-RACGP-Standards-for-general-practices-5th-edition.PDF>>

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

Royal College of General Practitioners, *Handbook for the Management of Health Information in General Practice 3rd ed* (2016)

Royal College of General Practitioners, *Standards for General Practices 4th ed* (2015)

Simrall, Sara Rorer, American Health Lawyers Association, *Social Media Compliance Challenges: From HIPAA to the NLRA, Social Media and HIPAA Privacy Concerns for Healthcare Providers*
<https://www.healthlawyers.org/Events/Programs/Materials/Documents/HHS13/Z_rorer.pdf>

Smith, Paul, 'Litigation, PR Disasters and Higher Insurance Costs Expected From New Data Breach Laws' *Australian Financial Review (Online)*, 10 August 2015
<<http://www.afr.com/technology/litigation-pr-disasters-and-higher-insurance-expected-from-new-data-breach-laws-20150805-gis75j>>

Smith, Paul, *There are some challenges, but in all, general practice is in a healthy space* (28 September 2016) *Australian Doctor*
<<http://www.australiandoctor.com.au/news/news-review/fighting-the-good-gp-fight-1>>

Social Media News, *Social Media Statistics Australia - October 2016*
<<http://www.socialmedianews.com.au/social-media-statistics-australia-october-2016/>>

Statista: The Statistics Portal, *Number of Social Media Users Worldwide from 2010 – 2020* <<https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>>

Trenholm, Richard, *Photos: The History of the Digital Camera* (6 November 2007) CNet <<https://www.cnet.com/au/news/photos-the-history-of-the-digital-camera/>>

University of Alabama of Birmingham Libraries: Reynolds-Finley Historical Library, *Percival Thomas (1740 – 1804)*
<<https://www.uab.edu/reynolds/histfigs/percival>>

World Medical Organisation, *WMA Declaration of Geneva* (2016)
<<http://www.wma.net/en/30publications/10policies/g1/>>