

Applying ethical and legal principles to new technology: the University of Auckland Faculty of Medical and Health Sciences' policy 'Taking and Sharing Images of Patients.'

Monique Jonas, Phillipa Malpas, Kate Kersey, Alan Merry, Warwick Bagg

ABSTRACT:

AIMS: To develop a policy governing the taking and sharing of photographic and radiological images by medical students.

METHODS: The Rules of the Health Information Privacy Code 1994 and the Code of Health and Disability Services Consumers' Rights were applied to the taking, storing and sharing of photographic and radiological images by medical students. Stakeholders, including clinicians, medical students, lawyers at district health boards in the Auckland region, the Office of the Privacy Commissioner and the Health and Disability Commissioner were consulted and their recommendations incorporated.

RESULTS: The policy '*Taking and Sharing Images of Patients*' sets expectations of students in relation to: photographs taken for the purpose of providing care; photographs taken for educational or professional practice purposes and photographic or radiological images used for educational or professional practice purposes. In addition, it prohibits students from uploading images of patients onto image-sharing apps such as Figure 1. The policy has since been extended to apply to all students at the Faculty of Medical and Health Sciences at the University of Auckland.

CONCLUSIONS: Technology-driven evolutions in practice necessitate regular review to ensure compliance with existing legal regulations and ethical frameworks. This policy offers a starting point for healthcare providers to review their own policies and practice, with a view to ensuring that patients' trust in the treatment that their health information receives is upheld.

Technology is developing at a breath-taking pace across social and professional domains, and medical practice is no exception. New technologies create exciting possibilities for providing and documenting care, and for interacting with patients and colleagues. Some may enable streamlining and improvement of models of care in the New Zealand health system. There are many reasons to welcome technological developments in medicine.

However, the changes that technology engenders sometimes obscure the underlying ethical and personal dimensions of a given practice or interaction, making the application of legal and ethical guidelines less clear.

This report presents the policy that the medical programme at the University of Auckland has developed to address the emergence of apps that enable patient images to be shared with an international audience. The policy now applies to all

healthcare students at the Faculty of Medical and Health Sciences (FMHS). Image-sharing apps and social media sites that allow image sharing raise issues about patient confidentiality, privacy, consent and what is permissible and expected within the provider-patient relationship. New Zealand has established professional guidelines and legal mechanisms that set expectations for how healthcare providers treat patient information, including the use and dissemination of images. As technology changes practice, however, reviews are necessary to ensure compliance with existing ethical and legal principles.

This policy applies the principles contained in the Code of Health and Disability Services Consumers' Rights 1996 (the Code of Rights)¹ and the Health Information Privacy Code 1994 (the HIPC)² to the taking and sharing of photographic and radiological images of patients. Some health and disability care providers (providers) have policies that deal specifically with images,³ and others are developing them,⁴ but it is likely that some are yet to address this area of practice. The Australian Medical Association has issued guidance for medical students and doctors about the use of personal mobile devices to take images, although it does not explicitly address image-sharing apps.⁵ The policy presented here is aimed at students, but may be relevant to providers considering their practices in the light of new technologies.

Background

The initial impetus for this policy was anecdotal evidence of an increasing awareness among medical students of a medical image-sharing application (app), Figure 1. It became clear that the ethical questions raised by electronic image-sharing also apply to related practices, and that the FMHS needed a policy to set expectations around the taking and sharing of patient images.

Figure 1

Figure 1 is currently the most prominent app enabling healthcare providers to share patient images, although many other platforms exist. According to its website, Figure 1 has over one million users internationally.⁶

It is freely available for anyone to download, and enables users to upload photographic and radiological images for other users to view. Explanatory notes, observations or questions can be added. Users who self-identify as healthcare providers (including nursing and medical students) can leave comments about images.

Figure 1 was conceived as a device to facilitate medical education and knowledge-sharing, and the discussions associated with various images on the website suggest that it offers a valuable forum for these purposes. Consulting with and learning from colleagues are important aspects of medical education and quality improvement.⁷ The inclusion of radiological and photographic images in clinical case presentations is an established practice for this reason.

It may seem, then, that image-sharing apps and social media platforms do not fundamentally change medical practice: they simply facilitate certain aspects of it. However, new and probably unintended risks are introduced by the potential scale of the audience, the lack of any requirement to verify users' identity or their reasons for viewing images, and the lack of control that users have over the images they upload. The potential for patient rights to be breached through the uploading of images to apps is clear. Notably, rights to privacy and consent are at issue. Figure 1 has taken measures to limit violations of patient rights, and operates on the basis that privacy is preserved if the connection between individuals and information relating to them (in this case, in the form of images) is severed or weakened. In keeping with the relevant legislation in Figure 1's home jurisdiction, the US (the Health Insurance Portability and Accountability Act 1996 (HIPAA)),⁸ the app states that only de-identified images should be uploaded.⁹ The HIPAA places no limits upon the disclosure or use of de-identified health information, which is defined as information from which identifiers such as names, addresses and assigned personal identifiers have been removed, and which poses no more than a 'very small risk' of enabling recipients to identify the individual.^{10,11}

Figure 1 features software that recognises and blocks faces. Users can alter or edit images to obscure identifying features

such as tattoos. Moderators review images for identifiability before they are made available to view. There is a process for viewers to report images that they believe enable identification.

Health information and disclosure

In New Zealand, the HIPC sets out rules governing the collection, retention, use and disclosure of health information by agencies in the health sector, including health and disability service providers. Rule 3 requires that, when health information is collected from an individual, he or she is aware that the information is being collected (3(1)(a)), of the purposes of collection (3(1)(b)), the intended recipients (3(1)(c)), the names and addresses of both the agency collecting (3(1)(d)(i)) and the agency that will hold the information (3(1)(d)(ii)) and whether or not collection is mandatory (3(1)(e)), what consequences there are for the individual if information is not provided (3(1)(f)) and what rights of access to and correction of information the individual has (3(1)(g)).

Rule 11 of the HIPC sets limits upon disclosure of health information, and permits disclosure under certain circumstances. Rule 11(1) established seven grounds upon which an agency may disclose health information, including that the individual concerned (or their representative) authorises disclosure (11(1)(b)); or that disclosure is connected to a purpose for which the information is obtained (11(1)(c)). Rule 11(2) allows for unauthorised disclosure 'if the health agency believes on reasonable grounds that it is either not desirable or not practicable to obtain authorisation from the individual', and one of eight further conditions apply. 11(2)(a) is that disclosure is connected to a purpose for which information was collected; 11(2)(c) is 'that the information is used in a form in which the individual concerned is not identified.' This suggests that sharing of patient images by providers could be permitted by HIPC, if the individual concerned has authorised it, or that 'it is not desirable or practicable to obtain authorisation' (11(2)), and the individual is not identifiable (11(2)(c)(i)).²

Right 1(2) in the Code of Rights establishes that: 'Every consumer has the right to have his or her privacy respected.' Privacy is defined as 'all matters of privacy in respect of the consumer', excepting three parts of the Privacy Act (relating to complaints (x), information-matching (viii) and public registers (vii)).¹ However, the Office of the Health and Disability Commissioner confines its consideration of possible breaches of Right 1(2) to matters pertaining to physical privacy, placing informational privacy entirely within the jurisdiction of the Privacy Commission.¹² Thus, Rule 11 of the HIPC provides the best guide to the legal requirements for image-sharing by providers.¹³

Privacy

The HIPC was written before image-sharing apps emerged, and thus does not directly address them. In the absence of specific guidance, providers contemplating uploading images on any electronic site must interpret how the HIPC's rules apply to their proposed practice. Whether image-sharing without patient authorisation is permissible is likely to depend upon the success of de-identification, but the HIPC does not specify what is required to meet the requirements of Rule 11(2)(c)(i). De-identification is not necessarily straightforward. Visual recognition is a form of identification that can survive the stripping of information such as names or personal identifiers. Whether an individual can be identified from an image can depend upon who is viewing it. In a case note relating to the Information Privacy Principles under the Privacy Act 1993,¹⁴ (rather than the HIPC) the Privacy Commissioner considered that an image with a man's face obscured was not identifiable, as there was no "distinctive feature or a personal connect of some kind".¹⁵ This suggests that photographic images of an individual may not be regarded as inherently identifying. However, what constitutes a 'distinctive feature or personal connect' may be position-specific. Features that might not be regarded as distinctive to strangers may allow close personal associates to recognise an individual. Difficulty surrounding de-identification is amplified by the fact that some images contain potentially identifying features because the person in

question has an unusual condition in which those features are implicated. This can mean that parts of a body that wouldn't normally enable identification are identifying. While Figure 1 succeeds in severing the connection between many of the images it displays, and the imaged patient for most viewers, some including several images of children, could enable identification by a personal associate. The lack of definitive guidance about how identifiability is to be understood in the context of the HIPC makes app-enabled image-sharing by providers legally risky.

Consent

The HIPC allows for use of identifying information if this is agreed to by the person to whom it relates. People can, and do, make personal information about themselves available to a wide audience on various social media sites (including YouTube, Facebook, Instagram, Snapchat, Tumblr, Reddit and Tinder), and some may be willing to have images shared for the purposes of promoting medical education and knowledge-sharing. Figure 1 provides jurisdiction-specific consent forms for providers, but users are not obliged to use them.¹⁶ The Terms of Service state that it is the provider's responsibility to ensure compliance with the legal and professional requirements in their jurisdiction, including those pertaining to patient consent:

*You are at all times solely responsible for obtaining and maintaining all patient consents, if applicable, and all other legally necessary consents or permissions required or advisable to disclose, process, retrieve, transmit and view the Patient Information that you transmit, store or receive in connection with the Site, Services, App and any third party site.*¹⁷

Patient consent is neither a simple nor a complete solution to ethical and legal concerns about image-sharing. Firstly, obtaining valid consent requires patients to understand the implications of their image being included in a global open forum such as Figure 1. Risks include those linked to being the subject of public ridicule, or of being identified, or of feeling compromised by a person in a fiduciary relationship. If a patient does not properly understand the nature of the forum the images are uploaded to, and the associated risks, any consent given may not be valid.¹⁸ Furthermore, even

if patient images are de-identified, uploading them to an open app is likely to violate reasonable patient expectations about the safeguarding of their health information. Loss of patient trust is a real possibility.

Trust

Even when consent is informed, questions about the appropriateness of the request remain. Patient trust in providers to put their medical interests first may be compromised through a request for permission to upload an image of them to such an open forum. Patients may feel uncomfortable about being put in the position of having to refuse what they regard as an improper request. The possible impact of such a request upon the doctor-patient relationship and upon overall trust in the confidentiality of health information should be taken into account by providers considering contributing material to image-sharing apps.

Control

Control of images is ceded, in perpetuity, to Figure 1 when they are uploaded.¹⁹ After uploading, neither the patient nor the provider can control where an image ends up, or to what uses it is put.

Although it is common practice for providers to show and discuss patient images at conferences and professional meetings, and to submit images for publications in professional journals, the audiences in these cases are predominantly restricted to health professionals. The audiences for apps like Figure 1 are unrestricted. Uncertainty about how apps will develop in the future compromises the specificity and reliability of information supplied as part of the consent process. It also makes it hard for providers and patients to weigh the benefits against the risks. The lack of guarantees or control accorded to uploaders raises questions about whether image-sharing via apps would comply with Rule 5(1) of the HIPC, which requires: "That a health agency that holds health information must ensure that: (a) the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against: (i) loss; or (ii) access, use, modification, or disclosure, except with the authority of the agency; or (iii) other misuse."²²

Although image-sharing apps build upon established practices, they also diverge

from them. It is crucial that the differences between established and emerging practices are recognised, and the ethical dimensions, responsibilities and legal ramifications of image-sharing via apps are accounted for.

Development of the policy

The Policy 'Taking and Sharing Images' was drafted through a process of applying the HIPC, along with the Code of Rights, to the practice of taking and using photographic and radiological images in a healthcare setting. Clinicians, medical students, lawyers at district health boards in the Auckland region, the Office of the Privacy Commissioner and the Health and Disability Commissioner were consulted through a variety of means: face-to-face meetings, Skype calls and group emails. As a result of the consultative process, the recommendations of key informants were incorporated into the policy.

A view was reached that it is not the proper role of a student to share patient information in the way enabled by apps such as Figure 1. This policy therefore prohibits students from uploading images to image-sharing apps.

The policy also contains guidance about taking and sharing photographic and radiological images of patients more generally. Technology is transforming the ways in which images are taken and stored in clinical practice. Technological advances enable improvements in patient care; for instance, photographs may facilitate the monitoring of a condition or the documentation of clinically significant features, and today these are easily stored within a patient's electronic record. However, technological advances also bring risk. It is now

easy to use personal devices such as smart phones to take photos or record information. This increases the risk of patient information being taken off-site and inappropriately shared or even lost.^{20, 5} Many people have devices that synchronise with other devices, sometimes automatically. This increases the risk that patient images taken or stored on personal devices may remain in the personal care of a provider, even after endeavours to remove them.

This policy applies currently accepted principles to present day practice to guide medical students in their use of images. Practices, technology and ethical norms all change over time, so this policy will require regular review and engagement with stakeholders. We hope that the policy document will stimulate discussion within our hospitals and universities, and in the correspondence section of the NZMJ. It may be appropriate to expand its scope as a result of such discussions and feedback, which we welcome.

The policy

Taking and sharing images of patients

There can be good reasons to take photographic and radiological images of patients. There can also be good reasons to allow certain others to view images. However, images are inherently sensitive parts of a patient's medical record. They must be treated in a way that acknowledges that sensitivity and supports the trust that patients put in the medical profession.

This guidance sets out the standards that the Faculty of Medical and Health Sciences (FMHS) expects students to meet when handling both photographic and radiological images of patients in all healthcare settings.

1. Generic principles

Images contain information about patients. Therefore, they are subject to the 12 Rules of the Health Information Privacy Code, which can be summarised as follows:

1. Only collect health information if you really need it.
2. Get it straight from the people concerned where possible.
3. Tell them what you're going to do with it.
4. Be considerate when you're getting it.
5. Take care of it once you've got it.
6. People can see their health information if they want to.
7. They can correct it if it's wrong.
8. Make sure health information is correct before you use it.
9. Get rid of it when you're done with it.
10. Use it for the purpose you got it.
11. Only disclose it if you have a good reason.
12. Only assign unique identifiers where permitted.

(<http://privacy.org.nz/news-and-publications/guidance-resources/health-information-privacy-fact-sheet-1-overview/>)

Students must follow these rules in all their dealings with health information, including taking and handling images of patients.

Students must comply with the policies of the relevant healthcare organisation when taking and handling images of patients. It is the responsibility of students to familiarise themselves with, and follow, relevant policies, and to complete the paperwork that is required by the relevant healthcare organisation, noting that different policies may exist in different healthcare settings.

2. Photographs taken for the purposes of providing care

Photographs can be useful for diagnosis, treatment and review of a patient's condition. As such, they can form an important part of a patient's medical record. Students may be asked to assist a member of clinical staff in taking a photograph for clinical purposes.

Photographs should be treated like all other information contained within a health record: as confidential. In addition, because the rules governing health information are complex and breaches have serious consequences, FMHS requires that students follow these rules:

1. Only take photographs of patients with the permission of a senior clinician with responsibility for a patient's care.
2. In most situations, patients should consent to photographs being taken of them, and their agreement entered into the record. The treating clinician is responsible for the consent process. If a student is asked to take a photograph of a patient, he or she must ask the clinician about the arrangements for consent.
3. Wherever possible, use a device or camera belonging to the relevant treatment unit or the supervisor to take images. This is to ensure that images are stored and documented according to the healthcare organisation's policies.
4. If an image is taken with a student camera or device, it is the responsibility of the student to ensure that the image is downloaded and deleted from the camera or device before the student leaves the healthcare site. Where devices are set to synchronise with other devices, special care must be taken to ensure that images are deleted from all devices.
5. Where possible, ensure that images do not allow patients to be identified by a person not involved in their care.

3. Photographs taken for educational and professional practice purposes

Photographs of patients can have benefits beyond that involved in patient care. Students may learn from photographs; professional practice can be improved through auditing involving photographs; professional practice can be enhanced through dissemination of experience and discussion about cases. These are benefits that photographs can contribute to, but they may not be of direct benefit to patients. This, combined with their inherent sensitivity, means that patient consent to a photograph's use for one of these purposes is vital.

Patients trust that those providing them medical care would not ask to photograph them unless there was good reason to do so. They also trust that photographs will be treated sensitively and confidentially. In order to warrant this trust, FMHS requires students to follow these rules:

1. Only take photographs for an educational or professional practice purpose with the permission of a University of Auckland supervisor with responsibility for the patient's care.
2. Only take images for an educational or professional practice purpose with the consent of the patient.
3. It is the responsibility of the student taking a photograph to ensure that the following information is given to patients when a request is made to take a photograph of them, and that the information is understood and agreed to by the patient:
 - The purpose that the photograph will be used for.
 - Who will have access to the photograph. This does not mean that patients need to know the names of individuals who will see photograph, but they should know the role in which individuals will have access (ie 'my supervisor', 'my lecturers'; 'my study group'; 'attendees at a conference').
 - The arrangements for destroying the photograph once it has been used.
 - Time frames for use and retention of the photograph.
 - Arrangements for storing the photograph.
4. It is the responsibility of the student taking a photograph to ensure that consent is properly documented in the patient notes. This includes noting the information provided to patients.
5. The patient has the right to see the photograph(s) that will be used.
6. The patient has the right to change his or her mind, in which case the photograph should not be used and should be deleted. This should be noted in the records.
7. Where possible, ensure that photographs do not allow patients to be identified by a person not involved in their care.
8. It is the student's responsibility to ensure that any photographs taken comply with DHB/PHO policy.
9. Photographs should only be shared selectively. Only those with whom it is necessary to share a photograph to meet the purpose for which consent was obtained should have access to the photograph.
10. A student who takes a photograph of a patient must take all reasonable steps to ensure that the image is treated in a respectful manner.

4. Using radiological and photographic images for educational and professional practice purposes

Students may wish to use existing radiological or photographic images (taken for the purposes of providing care) for educational or professional practice purposes. For instance, they may wish to include a copy of a scan or x-ray in a case report.

Radiological or photographic images are part of the patient's health care record, and should be treated according to the same principles as the rest of the record. Health care providers are responsible for abiding by the Health Information Privacy Code.

FMHS expects students to follow the following rules:

1. Students must have the permission of a clinician responsible for a patient's care before accessing and using a radiological image for educational or professional practice purposes.
2. Students must ask the clinician whether they should seek consent from the patient to use of the image. Whether an additional specific patient consent is necessary will depend upon factors such as the purposes for which the image was taken, and what the patient understood it might be used for. The clinician responsible for a patient's care must make the determination about whether or not patient consent should be sought.
3. Students must remove identifying information (names and NHI numbers) from the image.

Apps facilitating sharing of medical information

Apps such as Figure 1 enable images of patients to be accessed by anyone else in the world who has the app. Figure 1 offers no way to ensure that images are treated appropriately by the persons who access them. Images can be disseminated beyond the scope necessary to ensure that a given benefit is obtained. They allow comments to be made on images that could be disrespectful, hurtful and degrading of trust between doctors and their patients. Images uploaded to Figure 1 may not be easily removed from public view or public record. Because Figure 1 is available to non-health professionals, it offers little if any means of controlling dissemination of an image.

For these reasons, **students must not upload images to Figure 1** or to similar apps. If a student has any questions or concerns in relation to the taking and sharing of photographs of patients, they should contact a University of Auckland clinical supervisor or one of the authors of this guidance.

Competing interests:

Dr Merry reports affiliation with Safer Sleep LLC outside the submitted work; and is the Chair of Board of Health Quality and Safety Commission in New Zealand.

Acknowledgements:

We would like to thank the anonymous reviewer for their insightful and constructive comments. We also gratefully acknowledge the contribution of students and colleagues within FMHS and within district health boards who have advised and assisted with the writing of the Policy.

Author information:

Monique Jonas, Senior Lecturer, Faculty of Medical and Health Sciences, University of Auckland, Auckland; Phillipa Malpas, Senior Lecturer, Faculty of Medical and Health Sciences, University of Auckland, Auckland; Kate Kersey, Lecturer, Faculty of Health and Environmental Sciences, AUT, Auckland; Alan Merry, Professor, Head of School of Medicine, Faculty of Medical and Health Sciences, University of Auckland, Auckland; Warwick Bagg, Associate-Professor, Head of Medical Programme, Faculty of Medical and Health Sciences, University of Auckland, Auckland.

Corresponding author:

Monique Jonas, School of Population Health, Faculty of Medical and Health Sciences, University of Auckland, Private Bag 92019, Auckland.
m.jonas@auckland.ac.nz

URL:

<http://www.nzma.org.nz/journal/read-the-journal/all-issues/2010-2019/2017/vol-130-no-1449-27-january-2017/7136>

REFERENCES:

1. The Health and Disability Commission Code of Health and Disability Services Consumers' Rights Regulation 1996.
2. The Health Information Privacy Code 1994.
3. Waikato District Health Board Image Policy Committee. Information for patients available at <http://www.waikatodhb.health.nz/enquiries/guide-for-the-media/medical-photography/>
4. Nelson and Marlborough District Health Board. Minutes of Public Meeting. 25 August 2015. Reported in <http://www.stuff.co.nz/nelson-mail/news/74398698/Privacy-concerns-prompt-health-board-to-develop-policy-on-cameras-in-hospitals>
5. Australian Medical Association, Medical Indemnity Industry Association of Australia. Clinical Images and The Use of Personal Mobile Devices: A Guide for Medical Students and Doctors. Available at <http://ama.com.au/article/clinical-images-and-use-personal-mobile-devices>
6. Figure 1 website. <http://figure1.com/>
7. Magin P, Morgan S, Wearne S, et al. GP trainees' in-consultation information-seeking: associations with human, paper and electronic sources. *Family Practice* 2015 32:525–32.
8. Health Insurance Portability and Accountability Act 1996.
9. Figure 1 website. <http://figure1.com/sections/identifiers/>
10. United States Department of Health and Human Services and Office for Civil Rights. Summary of the HIPPA Privacy Rule. Last revised 05/03. Available at <http://www.hhs.gov/sites/default/files/privacysummary.pdf>: p. 3
11. Code of Federal Regulations. 45 CFR 164.514 - Other requirements relating to uses and disclosures of protected health information.
12. Health and Disability Commission. Shared Electronic Health Records: The Management of Withheld Information in Today's Health Care Environment (A Discussion Document). Submission. 6 March 2015. Available at <http://www.hdc.org.nz/publications/other-publications-from-hdc/submissions/shared-electronic-health-records-the-management-of-withheld-information-in-today's-health-care-environment>. Accessed 21 May 2016
13. Tobin R. Healthcare and Privacy Law. In Penk S and Tobin R, editor. *Privacy Law in New Zealand*. Wellington; Brookers Ltd; 2010, p161–177.
14. The Privacy Act 1994.
15. Case Note 64131 [2006] NZPrivCmr7.
16. Figure 1. Frequently Asked Questions. How Do I Handle Patient Consent? <http://figure1.com/sections/faq/index.html> Accessed May 20 2016.
17. Figure 1. Terms of Service. 13 Patient Data and Legal Compliance. <http://figure1.com/sections/tos/>. Accessed May 20 2016.
18. Bagg W, Adams J, Anderson L, et al. Medical Students and informed consent: A consensus statement prepared by the Faculty of Medical and Health Sciences of the University of Auckland and the University of Otago Medical School, Chief Medical Officers of District Health Boards, New Zealand Medical Students' Association and the Medical Council of New Zealand. *New Zealand Medical Journal* 2015 128:27–35.
19. Figure 1. Terms of Service. 8 Ownership. <http://figure1.com/sections/tos/>. Accessed May 20 2016.
20. Ponemon Institute. Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data. Ponemon Institute May 2016.