In this issue

[Member Bulletin]
Foreword - Kevin Shaw - Vice President iappANZ
Privacy Practice - Leading by example
Health Information Privacy - Unpacking the EHR
Contact us

[Member Bulletin]

While iappANZ aims to provide its Members with timely and relevant information about what's happening in the Australia and New Zealand privacy environments, we are also aware that our membership is part of a unique community of practice – where access to practical strategies for accomplishing the tasks of a privacy professional are as valuable as a resource as the legal, academic and political discourse available through iappANZ and other sources.

The Member Bulletin is a monthly publication, exclusive to Members, that highlights the issues affecting today’s privacy professionals as part of their day-to-day business and points Members toward information and strategies that may assist them.

[Foreword:]

In recognition of the fact that it is often the little things that pack the biggest privacy punch, this month we highlight a few aspects of our day-to-day personal information handling that could be done better. We also take the time to reflect on some of the privacy considerations relating to securing personal information contained in electronic health records following recent media attention to this issue.

Kevin Shaw
Vice President
iappANZ Board

[Privacy Practice – Leading by example]

While it may seem trite to consider privacy in terms of dos and don’ts, there is relevance in having a look at practices we engage in every day to see if we can take steps towards handling personal information better. The following represents five areas of day-to-day business that are typical across most sectors, where commonly we are simply ‘getting on with
it’ and so may not recognise that even the smallest changes can go a long way toward privacy enhancement.

1. Customer service

**Taking complaints**

**What we could do better:**

☑️ Instead of hearing a person’s complaint at a customer service counter, consider using a ‘break out room’ or moving to a space outside of public view
☑️ When taking a complaint over the telephone, keep your voice down and avoid repeating sensitive personal details out loud wherever possible
☑️ Where appropriate, encourage people to make their complaints in writing and then follow up with them over the telephone at an appropriate time

2. Case management

**Trouble-shooting case details with your colleagues**

**What we could do better:**

☑️ Although the elevator, the washroom, the bus, train or airplane may be the only place you can catch your colleagues alone, avoid discussing the personal details of your clients in this space
☑️ If you are taking an important call on your mobile phone, and the caller is divulging sensitive details about a case/ client, turn your earpiece volume down – otherwise, everyone around you is likely to hear the conversation too!
☑️ Consider having 5-minute trouble-shooting meetings in a designated office space each morning and afternoon to discuss sensitive case details with your colleagues
☑️ Ask yourself: ‘Do I really need my colleague’s input on this?’ – after all, not everyone has a specific need to know

3. Board meetings

**Recording meeting minutes**

**What we could do better:**

☑️ If the meeting itself is being recorded (e.g. audio or audio-visual recording), as opposed to just the written minutes, it is best to inform all participants up front
☑️ Ensure the details of attending participants (e.g. name, position) are recorded correctly
☑️ Comments made about people or situations that are not relevant to the meeting may be best left unrecorded
☑️ Where possible, circulate the written minutes to all meeting participants to be ratified before the final version is circulated

4. Program development
Engaging service providers

What we could do better:

☑ In order to ensure stakeholders are aware of privacy issues up front, consider conducting a privacy scan or a privacy impact assessment about your proposed program in advance of engaging your service provider
☑ Seek legal advice about the reach of privacy protections where an overseas service provider is being considered
☑ Double check your contracts – Does the service provider know what their obligations are regarding safeguarding personal information?

5. Get the job done

Working from home

What we could do better:

☑ Carry documents containing sensitive information – personal and otherwise – on a password protected storage device
☑ Avoid sending work-related documents to and from your own personal email address, unless you can be certain the transmission is secure
☑ Ensure your at-home work space is secure from hazards to personal information, such as theft, damage or loss
☑ Before talking to the people in your personal life about what you’re working on this weekend (as opposed to being at a BBQ with them!), consider whether you may be inappropriately divulging someone’s personal information

Nicole Waterson
iappANZ Board Member

Health Information Privacy – unpacking the EHR

Recent media reports appeared in the IT sections of The Australian under the headline: “Commissioner to probe potential privacy breaches”. This was in reference to the court case surrounding the Vioxx anti-arthritis drug and the alleged behaviour of the large pharmaceutical company Merck & Co. The concerns raised by the Australian Privacy Foundation (APF) relate to accessing details from patients’ medical files without their consent.

The following is a review of some issues surrounding the use or potential misuse of electronic medical records.

Information kept by healthcare providers would normally be regarded as ‘sensitive’ information that has special provisions under Privacy law, e.g. National Privacy Principles NPP 10. Consent to collect sensitive information is normally granted when consulting a healthcare provider. Who can have access to this information is covered by principles on use and disclose
(e.g. NPP 2). Hence, sensitive health information needs to directly relate to the primary purpose of collection and can only be shared if the individual would reasonably expect this as part of their ongoing primary healthcare. There are some exceptions such as when an individual has granted specific consent to secondary use or it is necessary for medical research or public safety.

Sharing health information is a valuable contribution to health knowledge and advancement. It ensures an understanding of epidemics, regional phenomena, adverse drug reactions, health outcomes, etc. and forms an integral part of modern healthcare provision. Much of this can be achieved without identifying the individuals concerned.

Removal of all the identifiers is referred to in the media article as ‘de-identified’ data which can be shared with secondary users provided the established rules are followed. This raises a question about how you can be sure that the individual cannot be re-identified by other means, e.g. inferences contained in the information or matching with other data sets. As highlighted in the above media article, the APF want the Privacy Commissioner to review if the procedures and processes in place provide sufficient protection.

There is a National Statement on Ethical Conduct in Human Research by the National Health and Medical Research Council (NHMRC) that classifies data into three types: i) identifiable, ii) re-identifiable, and iii) non-identifiable. That is, claiming data is ‘de-identified’ may not be sufficient if there are ways of readily re-identifying the individuals concerned. Medical researchers have often stated that undue privacy concerns are stopping access to valuable information for legitimate authorised research. Surveys have shown that the majority of people are supportive of electronic records and will support medical research providing safeguards are in place. How to effectively protect data and ensure it is truly ‘non-identifiable’ is an active area of research and policy reform. The danger is that repetitive privacy breaches could quickly erode the necessary ‘trust’ that individuals currently have with their healthcare service providers.

The issues raised above apply regardless of whether the information is in written or electronic form. The growing adoption of electronic health records will require a shift in the approaches taken. Electronic records provide a significant advantage in terms of convenience, health knowledge and, above all, medical safety. That said, the risks are different. With electronic data, the ability to access large volumes of data at high speed by unauthorised third parties requires new safeguards.

If the proposed new Unified Privacy Principles (UPPs) are adopted, as recommended by the Australian Law Reform Commission, then the requirement to ensure consent for collecting and sharing sensitive information will be mandated. That is, the proposed Collection principle UPP 2.5 differs from NPP 10 by removing the specific subclause (10.2) that allowed collection by organisations when the information is considered necessary to provide a health service. This implies that in the future the onus may well be with the collector and user of health information to demonstrate the individual has given explicit consent. The relevant technology used may need to track this consent together with an audit of all access made to records in a way that does not necessarily happen now.

In the light of this, it is perhaps not too surprising that the recently formed National Health and Hospital Reform Commission advocates in a recent supplementary paper that a personal health record that gives individuals ownership and direct control over who has access to their
information, such as those offered by Microsoft, Global Health and Google, may be the viable way forward for minimise privacy breaches.

As with many current and emerging privacy issues, it appears there is no simple definitive solution that can be applied. With Health Privacy, as with so many privacy issue areas, it is about seeking consultation and striking the right balance.

Dr Peter Croll
iappANZ Board Member

If you have any comments or suggestions about this newsletter or any other aspect of the iappANZ please contact us. Do you have interesting articles or information you would like to share with Privacy Professionals - let us know....contact us at the iappANZ office.

Email: admin@iappANZ.org
Web: www.iappANZ.org
Phone: +61 3 9895 4475
Fax: +61 3 9898 0249
Mail: PO Box 193
      Surrey Hills Victoria
      Australia 3127

This email has been sent by the International Association of Privacy Professionals (ANZ).
To unsubscribe from this mailing list, click here.