Australian
Privacy
Foundation

http://www.privacy.org.au
Secretary@privacy.org.au
http://www.privacy.org.au/About/Contacts.html

20 October 2015

Kate Deakin

Adviser, Health and Privacy Assessments
Regulation and Strategy Branch
Office of the Australian Information Commissioner
GPO Box 5218 SYDNEY 2001
kate.deakin@oaic.gov.au

Dear Ms Deakin

Re: Feedback on OAIC draft health privacy resources for health service providers and consumers

This submission by the Australian Privacy Foundation (the APF) is in response to requests by the OAIC for comments on new draft health privacy resources for health service providers and consumers.

It follows previous APF submissions on health privacy which are available on-line, a selection of which are detailed at the end of this submission.

Standing of the Australian Privacy Foundation

The Australian Privacy Foundation (the APF) is the nation's premier civil society organization concerned with privacy.

Its membership includes lawyers, academics, information technology experts, health informatics fellows, communication policy analysts and non-specialists. It has been recognised through invitations to provide testimony in parliamentary inquiries and other consultations regarding data protection, along with participation in high-level international fora. A brief backgrounder is attached.

Comments

It is our view that it is very important that Australia has a well understood and accepted national framework for EHR privacy, confidentiality, information security and access control, appropriate for clinical outcomes for public and private health.

If we fail in this objective (as there appears to be the potential for happening) we are at risk of both undermining confidence in the core confidentiality and trust at the heart of the clinical relationship, and also of jeopardising the integrity, accuracy and fitness for sensitive purposes of the information -

especially if too many conflicting external data-mining motives have been allowed to overwhelm the core secure and controlled clinical record keeping of traditional systems.

We also note that the PCEHR in particular, which plays an unresolved, partly redundant, conflicted and potentially disruptive part in the EHR system, has been dogged by governance, security, accountability and trust issues due to its confused and conflicted strategic direction and attitude to patient consent and control -- so this personal health information area remains a live issue for all Australians.

Our submission is not an exhaustive treatment, as we have decided to focus on a few key points, mainly associated with the nature of health information and issues surrounding the correction of this information.

We refer to the guideline "Correction of health information by health service providers"

Our first comment refers to the section "When to correct personal information" and is associated with the concept of information consistency. When a service provider aggregates data from a number of sources it is possible that the information so aggregated may be inconsistent. We contend that, under these circumstances, the service provider should be required to, as a minimum, inform the various holders of the source information that there are issues of inconsistency. Other options are to identify who is required to resolve this inconsistency. Should it be the service provider or one of the holders of the source information, in which case what are the guidelines? We do not claim expertise in this area however we do believe it is a potential issue.

Our second comment refers to multiple sections "When to correct personal information"

> APP 13 requires you to take reasonable steps to correct personal information you hold about a patient if it is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to the purpose for which it is held.
>
> This requirement applies where:
>
> - you are satisfied the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, independent of any request from a patient, or
> - a patient requests you to correct the information.

and "When is information 'incorrect'?"

> "You must correct the personal information you hold when it is inaccurate, out-of-date, incomplete, irrelevant or misleading ('incorrect')."

and "Correcting information on your own initiative"

> You are required to take reasonable steps to correct personal information you hold if you are satisfied, having regard to a purpose for which the personal information is held, that it is incorrect.
>
> You are not required to check personal information you hold continually, however, you should be alert to the possibility that it may be incorrect and require correction. You may become aware information is incorrect in a variety of ways, for example where there is an inconsistency with other information; you are informed by another party that it is incorrect; or through practices,

procedures or systems implemented in compliance with APP 1.2 that detect incorrect information.

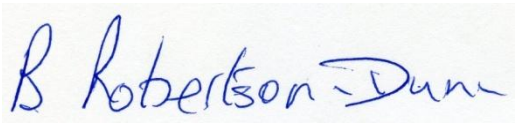
The issue we see concerns the different roles of service providers. Some may hold health information but have no expertise in determining if it is incorrect. Others may have expertise that allows them to make judgements regarding the correctness of health.

The phrases that concern us in this guideline are “if you are satisfied it is incorrect” and “You are not required to check personal information you hold continually, ...”.

We feel that there should be some obligation on service providers who create information on a patient, through tests or as the result of consultation, to proactively ensure that it is correct, especially with respect to other information they hold on that patient.

Thank you for giving us the opportunity to comment on these guidelines.

Yours sincerely



Dr Bernard Robertson-Dunn
Chair, Health Committee
Bernard.Robertson-Dunn@privacy.org.au

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html

- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following are some of the submissions previously provided to the OAIC

APF submission - eHealth record system OAIC Enforcement Guidelines.
https://www.privacy.org.au/Papers/OAIC-PCEHREnf-120924.pdf

Guidelines for developing codes
Issued under Part IIIB of the Privacy Act 1988 – Consultation draft Submission to the Office of the Australian Information Commissioner April 2013
https://www.privacy.org.au/Papers/OAIC-CodeDevG-130415.pdf

Improving OAIC's Privacy regulatory action policy
Submission to the Office of the Australian Information Commissioner (OAIC) 31 March 2014
https://www.privacy.org.au/Papers/OAIC-RegPolicy-140331.pdf

eHealth record system (PCEHR) Data Breach Notification, Submission to OAIC (29 Sep 2012)

eHealth record system (PCEHR) Enforcement Guidelines, Submission to OAIC (24 Sep 2012)

Guide to Privacy Regulatory Action, Submission to OAIC (12 Dec 2014)

OAIC's Draft Guide re Privacy Impact Assessments, Submission to OAIC (31 Mar 2014)