



**Australian  
Privacy  
Foundation**

G.P.O. Box 1196  
Sydney NSW 2001  
enquiries@privacy.org.au

<http://www.privacy.org.au/>

Rose Ross  
Director (a/g) Medicare Integrity Section  
Medicare Benefits Branch  
Department of Health and Ageing  
GPO Box 9848  
Canberra ACT 2601

26 November 2008

Dear Ms. Ross,

*Re: Stakeholder feedback about the “Increased MBS Compliance Audits” information sheet*

I am writing in my capacity as Chair of the Health Sub Committee of the Australian Privacy Foundation (APF) and refer to our letter to Senator Hockey of September 17, 2008, where the APF advised it was pleased to establish effective dialogue with the Medicare staff and the Department of Health and Ageing on pertinent matters.

We also note Mr. Peter Halladay’s request of November 14 2008, for feedback as to the information sheet “Increased MBS Compliance Audits”. The Foundation is generally supportive of departmental moves to require practitioners to verify their claims for Medicare eligible services as a reasonable and responsible way of ensuring that taxpayer funds are spent appropriately. Yet we remain concerned about the potential for privacy breaches.

We are especially concerned about the following changes:

**Access to evidence**

Medicare’s engagement in protracted negotiations with medical defence unions, industry bodies and legal firms, along with related administrative workloads do not

justify privacy breaches across the health sector. We support the idea of establishing legislative frameworks ratifying practitioner rights and obligations. However, organisational ease of audit does not justify threatening patient rights as to the privacy of their sensitive health information. The paper is quite general when it comes to the types of information it will require for audit. Also, one does not need unfettered access to patient data in order to breach their privacy- a label can be enough (e.g. Item 16590 might be a very shameful service to receive if one is a single Greek girl aged 15 years). In the end, for patients it is all about context, and when their identified or identifiable health records can be made available to a public authority for audit purposes, then that authority has betrayed public trust.

The paper also talks about appropriate safeguards for the collection and use of health information. Several information breaches, due to human error, have been recently reported in the press. What are the appropriate safeguards for human error? As time goes by, the scope for human error changes as technologies do. Medicare cannot guarantee the security of patient information. Therefore, restrictions confining access to times of reasonable suspicions of illegal behaviours after all other options have been properly considered, as well as the imposition of biting sanctions to dissuade abuses, as the recent ALRC report indicates, must be part of the audit system [*ALRC Report 108: For Your Information: Australian Privacy Law and Practice* 2008. [http://www.austlii.edu.au/au/other/alrc/publications/reports/108/\\_3.html](http://www.austlii.edu.au/au/other/alrc/publications/reports/108/_3.html)].

Finally, after discussing new training requirements and a legislative framework within which to ask for access to patient records, the “Increased MBS Compliance” information sheet claims this is not more red-tape for providers. Yet the *Medical Observer* has recently printed a series of two articles entitled “Medicare crackdown: Your survival guide” [Hoffman, L. Oct 31 & Nov 7 2008 <http://www.medicalobserver.com.au/medical-observer/Default.aspx>] to support clinicians through the change despite their concerns about resulting quality of patient care outcomes [Bracey, A. “Tougher penalties flagged for Medicare offenders” Nov 21, 2008 <http://www.medicalobserver.com.au/medical-observer/Default.aspx>]. The article refers to a requirement for doctors to store defensive patient records to support all Medicare claims. The audit process extends Medicare’s powers to review documentation from broader range of clinicians’ than at present. Logically then, the new audit process amounts to more red tape.

Furthermore, who will provide privacy and security training and to what benchmark? Australian health services and authorities have a very poor record when it comes to training individuals about privacy and security safeguards (see, for instance, Fernando & Dawson (2008) Clinician assessments of workplace security training- an informatics perspective, *electronic Journal of Health Informatics* (eJHI), 3(1) 27). The proposed penalties section does nothing to alleviate these concerns. Also, the discussion paper refers to Commonwealth legislation, which contradicts several other jurisdictions (ALRC op.cit.). Hence, the APF requires more specific detail for the argument presented in the Medicare paper in order to be convinced of governmental strategies to protect privacy and patient-doctor confidentiality.

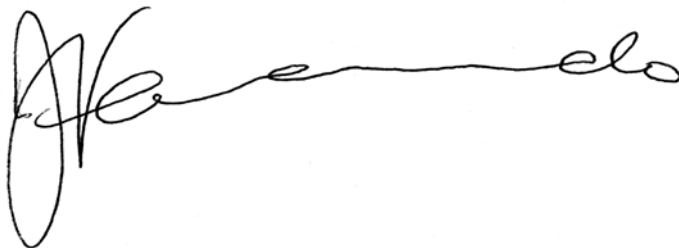
### **Legislative changes required**

A PIA must precede any legislative changes to the Health Insurance Act 1973.

### **Consultation**

The APF is a key stakeholder in the outcome of this proposal. We support revised ways of ensuring that taxpayer funds are spent appropriately, reasonably and responsibly. However, from a privacy and security perspective, the process outlined in the paper is intrinsically flawed. Consequently, we would be pleased to participate in ongoing consultation processes until a Medicare Audits Bill is satisfactorily introduced to Parliament.

Yours faithfully

A handwritten signature in black ink, appearing to read 'Juanita Fernando', written in a cursive style.

Juanita Fernando

Chair  
Health Sub Committee  
Australian Privacy Foundation  
GPO Box 1196 Sydney NSW 2001

email: [mail@privacy.org.au](mailto:mail@privacy.org.au)

web: [www.privacy.org.au](http://www.privacy.org.au)