NEW ZEALAND COUNCIL OF TRADE UNIONS
Te Kauae Kaimahi

Submission of the New Zealand Council of Trade Unions Te Kauae Kaimahi

to the

Independent Review of ACC Privacy and Security of Information

P O Box 6645
Wellington

7 June 2012

1.1. This submission is made on behalf of the 39 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU). With 350,000 members, the CTU is the largest democratic organisation in New Zealand.

1.2. The CTU acknowledges Te Tiriti o Waitangi as the founding document of Aotearoa New Zealand and formally acknowledges this through Te Rūnanga o Ngā Kaimahi Māori o Aotearoa (Te Rūnanga) the Māori arm of Te Kauae Kaimahi (CTU) which represents approximately 60,000 Māori workers.

1.3. While we appreciate the opportunity to make this submission on this important subject, it is brief because of the short time available. We would welcome the opportunity to provide further details.

1.4. This submission is under paragraph 1.3 of the terms of reference document (*Independent Review of ACC Privacy and Security of Information*). The relevant objectives are to:

> Determine if ACC's policies and practices relating to security of information are:
>
> - Appropriate (including comparability with private sector practices, consistent with good practice in the public sector and the health sector, appropriateness in terms of the risk related to the nature of the client data/information maintained by ACC)
>
> - Effective (in the context of addressing staff and clients need for access to information, maintaining confidentiality and privacy, communication, compliance, monitoring and culture of the organisation).

1.5. Some of the CTUs concerns were raised at the Stakeholder Consultation held on 29 May 2012. At that consultation, participants were invited to make further written submissions no later than 7 June 2012.

1.6. At the stakeholder consultation, the CTU representative spoke to a number of points raised in the general discussion. These and some additional points include:

- The importance of limiting information gathered to what is strictly necessary for the investigation and management of a person's claim.

- A specific issue was raised with respect to the ACC167 consent form which contains an 'etc' and implies a right to seek information without apparent limit. The extract reads as follows:

> "this consent applies to all aspects of my claim, and includes external agencies and service providers such as general practitioners, specialists, employers etc from whom ACC asks for information"

- The CTU spoke in support of keeping medical and administrative information separate on claim files with limited rights of access to the former (eg to other medical practitioners, medical advisors and senior technical claims staff only)

- In support of investigation of the feasibility of a secure portal system to allow safe and easy client access to claim information, as well as electronically audited ACC access.

- The importance of ensuring ACC's computer system allows for seamless incorporation of emails and other forms of correspondence to ensure files are always complete and accurate. At the moment, there appears to be discretion as to what information is stored within the EOS system, and how. When correspondence is omitted, this can have a bearing on issues under judicial review and potentially impede natural justice.

- Allow corrections of files (including injury description corrections) to be achieved more easily and for that to be easily audited. For example, where an ACC client has sought correction of an aspect of a file, this should be tracked and confirmed to the client with the correction prominently displayed. This can be material when the nature of an

injury is under dispute and there exists an incorrect or superseded injury.

- Address and standardise the timeliness of information delivery to ensure that information is provided and received as soon as practicable. While the spirit of the Privacy Act 1993 and the Health Information Privacy Code 1994 is that information should be provided as soon as practicable, some organisations currently make use of the letter of the Act and Code to mean they can wait a full 20 working days before responding to a request for information, rather than endeavouring to deliver it within a reasonable timeframe. While requiring steps to be taken "as soon as reasonably practicable", the relevant provisions in the Privacy Act and the Code allow up to 20 working days for *responding* to information requests rather than *delivery* within that period. It should be recognised that advances in electronic communications have radically transformed the information management environment since 1993 and that aspects of the Act may now be outmoded. In practice, technological tools allow for speedier turnaround, and ACC usually deliver files well within the 20 working day timeframe. The Act should be changed to stipulate more timely delivery with sanctions for failure to comply[1]. In the meantime, we would strongly recommend formalising guidelines for acceptable practice that incorporate a requirement for response and delivery to be as soon as is practicable but no later than 20 working days. Timely provision of files is often critical when ACC clients are off work without income and awaiting advice based on their claim history. While a large public agency such as ACC can and has adopted its own practices to ensure timely delivery, the practice among the numerous Accredited Employers and their Third Party Administrators is highly variable and matters are even more difficult because a claimant is dealing with multiple agencies.

[1] . We note that reform of the Privacy Act 1993 is being considered and that it has been the subject of a Law Commission report ('*Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4').* We believe this is timely and that wider community and stakeholder input should now be sought to inform that process.

- Foster a culture of positive communication and responsiveness with ACC clients.

1.7. We asked the reviewers to include scrutiny of practices under the Accredited Employer Programme within the above terms of reference. Accredited Employers are referred to within the Health Information Privacy Code 1994. Reference is also made to their legislative obligations under the Accreditation Agreement signed by each employer with ACC. Under that agreement, Accredited Employers effectively step into the shoes of ACC.

1.8. We consider aspects of the programme present unique challenges for the protection of workers' privacy. This is so for a number of reasons:

- Accredited Employer sites are spread throughout the country and essentially act as autonomous units (albeit subject to ACC oversight and audit). This creates the potential for disparate systems and variability in methods of information management.

- Accredited employers perform two distinct roles: as "employer" and "accredited employer/ACC agent". However, "employment" and "ACC" related information is effectively gathered by the same entity and is sometimes stored on the same premises (particularly when the accredited employer is self-managed). This creates the potential for "function creep" of information and for conflict of interest to occur. While this potential is addressed within the audit system, we believe stronger measures are required to guarantee separation of employment and ACC related information and processes. See the attachment named *Employment - ACC Separation* for an instance where a case manager employed by a third party administrator – WorkAon – has raised the possibility of employment termination in the context of that person's ACC claim. It is a crucial underlying principle of the existing privacy legislation that information is only gathered for its stated purpose and that its integrity is protected (i.e. to avoid "function creep" and other inappropriate uses). We would like to see more robust oversight of information management practices of

Accredited Employers to ensure adherence to this fundamental principle.

- Note that recommendations made by the Office of the Privacy Commissioner to strengthen the audit standards in this respect were presented to ACC by the CTU but to date these have not been taken up: see attached document *PP Draft '30 Sept – with OPC Tracked Changes*, p 34 and 35.

- Related to the above, there is potential for confusion of roles with regard to the management of claims and access to private claim information. For example, when a workplace injury occurs, staff involved might variously include Human Resource and/or Health and Safety personnel, general management staff, supervisors, team leaders, administration staff and a case manager.

1.9. Specific concerns that have been raised by unions with respect to Accredited Employers and with relevance to the privacy legislation include:

- Accredited Employers seeking broad, non-specific access to all medical information and the potential misuse of this information.

- Unnecessary and apparently deliberate delays in providing requested file information by some accredited employers. A case history is available on request to illustrate this issue.

- A mandatory requirement by some employers for workers to attend employer designated GPs for the management of their claim and ongoing care.

- Supervisory staff actually accompanying workers into consultations with these designated doctors (as a mandatory requirement).

- Unauthorised cross sharing of medical information by doctors acting in multiple capacities with possible conflicts of interest. For example, a doctor may act both as the employee's health provider (subsidised by the employer) and as the Accredited Employer's medical advisor in the

context of the claim. Again, a case study demonstrating this issue is available if required.

1.10. In summary, in addition to the changes outlined above relating specifically to ACC, the accredited employer scheme requires special attention. There is an imbalance of power in this context which includes the role of the non-treating doctor (who is contracted to the employer), the employment relationship, and often the lack of real choice injured employees have in giving their employer informed consent to access their private medical information. This creates circumstances that demand stronger measures to ensure that an employee's private medical information is protected.

1.11. Accredited employers potentially have unfettered access to medical information, and often have available to them information that would not normally be made available to other employers. This can then be used against workers in the context of the employer/employee relationship, leading to dismissals for medical frustration of contract. Sometimes it appears there is little separation between administration of the partnership scheme and corporate Human Resources functions, and a lack of appreciation that information received for one purpose should not be put to other purposes.

1.12. This is an area where serious misuse of private medical information can occur and, while ACC provides oversight to AEs on matters relating to work injury claims, these issues must be systematically addressed.