



# interRAI computer safety and privacy guidelines

## Information for assessors, administrators and managers

---

### Section A: Use of interRAI – Privacy / Security Considerations

When you access the national interRAI system you are accessing client related health information. Although this is a nationally hosted system you and your organisation's obligations under the Privacy Act of 1993 and the Health Information Privacy Code remain.

**You are reminded that your use of the interRAI software may be subject to audit and that the software keeps a full audit trail of your access. Therefore please remember to only access and use information that is necessary for the performance of your duties.**

**If by audit this is found not to be the case, your access to interRAI may be suspended pending further investigation and that inappropriate access may result in a disciplinary process.**

**Please ensure that you understand your obligations when accessing health related information with regard to the Privacy Act of 1993, the Health Information Privacy code of 1994 and all subsequent amendments thereof.**

The national system has a comprehensive audit trail of activity undertaken on the system and this is linked to your login ID. Even if you view a record via the client/client overview screen and do nothing else with that record, the access to the client/client overview screen is logged as 'Record Viewed' on the audit reports.

As a number of entities come together within a local model of care to provide continuity of care for a client/client, organisations are asked to establish local transparent processes to ensure a level of proactive access audit occurs. The local interRAI systems clinician can help establish this process.

## Section B: Basic Computer Security and Access to the System

As a generic security measure, this system has an automatic time out for prolonged periods of inactivity such that, if you have not clicked on a link or a button within the application of 90 minutes, the session you are logged into will expire. This is a similar setting to many other systems, eg internet banking, though the setting in these systems is generally lower at 10-15 minutes.

Please follow these basic guidelines:

1. Do not share your passwords or login IDs and do not leave your login ID or password written down anywhere that other people can see.
2. Ensure your password is not easy to guess or work out from other information people may know about you.
3. Do not enable the auto-complete setting on your browser for the log in page to the interRAI.
4. Do not click on website links sent to you in emails unless you are completely sure of the source and know it can be trusted.
5. Do not access the system from public computers that you do not know are secure, for example an internet café or a public wi-fi.
6. Do not leave your computer unattended and logged in (note the system has a 90 minute time out set so that if no link or button is clicked for 90 minutes, your session will be logged out).
7. Do not leave your computer unattended in a public place (or in your car).
8. Forward any suspicious emails you get to the interRAI Service Desk
9. If in doubt call the helpdesk.
10. Assessment to be 'Checked-Out' mode on the laptop for a maximum of 72 hours.
11. An assessment is to be marked 'complete' three working days after the assessment has been undertaken with the client.

**Treat the computer like you might treat your wallet/purse.**