National E-Health Transition Authority (NEHTA) Checklist

My Health Record System Security Policy	✓ The organisation has a My Health Record system security policy in place ✓ The policy is communicated to all staff and is readily accessible to all staff and any healthcare providers to whom the organisation supplies services under contract ✓ The policy is enforced in relation to all staff ✓ The policy is regularly reviewed (at least annually) to ensure relevance and accuracy, in particular where any new material or changed risks are identified and where changes in eHealth legislation or the structure of the organisation occur ✓ Each iteration of the policy contains a unique version number and the date when that iteration came into effect ✓ The organisation is able to provide a copy of the policy on request to the System Operator within 7 days ✓ The policy sets out: • The organisation's user account management measures and manner of authorising staff to access the My Health Record system (see 'Managing User Accounts') • The training that will be provided to users who access the My Health Record system (see 'Staff Training') • The process for identifying staff who request access to the My Health Record system (see 'Identification of staff') • The process for destroying My Health Record system document and record codes in a secure manner The mitigation strategies to ensure My Health Record system related security risks can be identified, acted upon and reported (see 'Handling of Privacy Breaches and Complaints' and 'Risk Assessments')
Managing User Accounts	✓ The names and position of staff who are authorised to access the My Health Record system are recorded and kept up-to-date ✓ Practice software controls limit access to the My Health Record system to those staff required by the duties of their role to access the system ✓ Staff are provided a unique user account with individual login ✓ Staff passwords are regularly reviewed, changed and sufficiently complex ✓ Users are required to enter their user name and password to deactivate screensavers ✓ A user account is immediately suspended or deactivated where a user leaves the organisation, has the security of their account compromised or whose duties no longer require them to access the My Health Record system ✓ A user account is inactivated/deleted after the departure of staff members as part of the organisation's off-boarding process ✓ Where My Health Record system Provider Portal access is required, the organisation maintains a list of up-to-date authorised providers and communicates this with the System Operator
Identification of Staff	✓ Clinical software is used to assign and record unique internal staff member identification codes (including an HPI-I for those providers with an HPI-I) ✓ The unique identification code, or the provider's HPI-I, is recorded by the clinical software against any My Health Record system access
Staff Training	✓ All staff requiring My Health Record system access undergo training before accessing the system ✓ Training is provided in relation to how to use the My Health Record system accurately and responsibly, the legal obligations on organisation and individuals using the system and the consequences of breaching these obligations ✓ Training is provided to staff on a regular and ongoing basis ✓ A register of staff who have attended training is maintained
Handling of Privacy Breaches and Complaints	✓ The organisation has a reporting procedure to allow staff to inform management regarding any suspected security or privacy issue or breach of the My Health Record system ✓ An incident register/log is kept of any suspected breach including details of the date and time of the breach, the user account that was involved and which patient's information was accessed (if known) ✓ A process is in place for the RO or OMO to report a breach to the System Operator ✓ If a patient raises an issue in relation to unauthorised access to their digital health record, the organisation has a complaints management process to take steps to investigate the issue
Risk Assessments	✓ The organisation undertakes periodic, privacy and security risk assessments of staff use of the My Health Record system and the organisation's ICT systems generally, and implement improvements as required ✓ All risk assessments are documented appropriately

Country SA PHN gratefully acknowledge the financial and other support from the Australian Government Department of Health.