



Smart Health

SOLUTIONS

ETHICS CHARTER SEPTEMBER 2005

NOTICE: The information contained in this document and any attachments is copyright and the property of Smart Health Solutions.

Security, Ethics and Privacy Principles

The requirement for security and privacy of patient clinical and other health information derives principally from:

- The National Privacy Principles (effective 21 December 2001),
- Various state privacy legislation and
- Ethical business practice.

Smart Health has been committed to the security, privacy and ethical use of patient health information since it commenced the development and live operation of secure on-line solutions for patient health information in 1999.

This commitment includes:

- Voluntary participation by patients and healthcare providers
- Informed consent to participate by patients
- Authenticating healthcare provider access to patient information
- Authenticating administrative access to patient information
- Patient authorisation of provider access to patient information
- Access to patient information that is strictly based on existing healthcare practice information management arrangements
- Securing repositories of patient and provider information
- Adherence to standards

- a. Voluntary participation by patients and healthcare providers

All patients and healthcare providers participate in the scheme on a voluntary or opt-in basis.

- b. Informed consent to participate by patients

Smart Health Solutions Pty Ltd
www.smarthealth.com.au

PO Box R248 Royal Exchange Sydney NSW 2000 • 39 Phillip Street Sydney NSW 2000 Australia
Phone +61 2 9247 3799 • Fax +61 2 9247 3899
ABN 34 092 690 670

All patients that participate in the scheme must acknowledge terms and conditions that are provided as part of the enrolment documentation.

c. Authenticating healthcare provider access to patient information

Authentication of access to patient information by healthcare providers is implemented using secure tokens and PKI provided for this purpose by the Commonwealth.

d. Authenticating administrative access to patient information

Authentication of access to patient information by healthcare providers is implemented using secure tokens and PKI provided for this purpose by the Commonwealth.

e. Patient authorisation of provider access to patient information

Healthcare providers only obtain access to patient information when they are explicitly authorised by the patient.

f. Access to patient information that is strictly based on existing healthcare practice information management arrangements

Providers are assigned to role based groups for the purposes of defining common access rights to patient information.

g. Securing repositories of patient and provider information

The scheme server and data repository (or repositories) is secured by locating it within a Gatekeeper accredited secure processing centre.