Australian Privacy Foundation

Policy Position

Protections Against eHealth Data Breaches

28 August 2009

http://www.privacy.org.au/Papers/eHealth-DataBreach-090828.pdf

Personal health data is by its nature highly sensitive, so unauthorised access and disclosure is of even greater concern than it is with other categories of data. Irrespective of what laws and norms might apply to data breaches generally, it is vital that clear and effective protections exist for personal health care data. The APF has accordingly adopted the following policy on the matter.

A **data breach** occurs when personal health care data is exposed to an unauthorised person, and there is a reasonable likelihood of actual or perceived harm to an interest of the person to whom the data relates.

1. **An organisation that handles personal health care data must**:

   (a) take such steps to prevent, detect and enable the investigation of data breaches as are commensurate with the circumstances

   (b) conduct staff training with regard to security, privacy and e-health

   (c) subject health care data systems to a programme of audits of security measures

   (d) when health care data systems are in the process of being created, and when such systems are being materially changed, conduct a Privacy Impact Assessment (PIA), in order to ensure that appropriate data protections are designed into the systems, and to demonstrate publicly that this is the case

2. **Where gounds exist for suspecting that a data breach may have occurred, the organisation responsible must**:

   (a) investigate

   (b) if a data breach is found to have occurred, take the further steps detailed below

   (c) document the outcomes

   (d) publish information about the outcomes, at an appropriate level of detail

3. **Where a data breach has occurred, the organisation responsible must**:

   (a) promptly advise affected individuals (and/or their next of kin or carers)

   (b) provide an explanation and apology to affected individuals

   (c) where material harm has occurred, provide appropriate restitution

   (d) publish an appropriate notice and explanation in a manner that facilitates discovery and access by people seeking the information

   (e) advise the Office of the Federal Privacy Commissioner

4. **Where a serious data breach has occurred, the Office of the Federal Privacy Commissioner must**:

   (a) review the outcomes of any investigation undertaken by the responsible organisation

   (b) where any doubt exists about the quality, conduct its own independent investigation

   (c) publish the results of the review and/or investigation

   (d) add the details of the data breach to a publicly available register, including any decision made as the result of the investigation, in order to ensure that information is available to support informed public debate about protections for personal health care data

5. **Where a data breach occurs that results in material harm**, the affected individuals must have recourse to remedies, both under the Privacy Act and through a statutory cause of action