Submission to :- My Health Record Enquiry

I am a private individual who has a passing knowledge of cyber security & a practical working knowledge of how easy security is to 'break' accidentally, either by laziness, stupidity or (perceived) convenience requirements.

With this in mind I would like to address a couple of issues in relation to the changes / existence of the My Health Record scheme.

1/ It is counter to basic privacy principles that this system be opt out rather than opt in.

2/ Records should be able to be deleted, not just suspended. Suspension should be an option in addition to full deletion.

3/ The **ONLY** people who should have access to these records for any reason are the record holder & their treating physician/medical professionals. As the systems reason for existence is to centralise **medical** reasons it is an immediate red flag that any other institution or person has access. This single point (other party access) is the most common reason people do not want the record.

It is my opinion that the only way the general public will support this system will be if the following conditions are met

a/ ONLY record holder & treating physician to have access. Nobody else – ever.

A secondary "This admission" record to be created for the general use of nurses etc. Under normal circumstances this to be the only accessible record. Record holder permission required for access to full record, eg secondary password or the like.

b/ Every record accessed to require login / confirmation of password to view. No log into system & stay logged in. EVERY record view to require login. Every 3rd page to require re entry of password.

This will ensure there are no data base breaches due to 'left logged in' etc.

c/ System MUST be opt in.

d/ Deletion option is a must

e/ If aggregated data is to be used for studies etc then a few conditions must be met

i) Every share of data MUST have positive permission of the record holder. Record holder must approve every share. There is NO IMPLIED APPROVAL.

ii) Those seeking access must :-

Be Australian based
Have been a listed entity for at least 5 years
Keep data totally within Australia – this includes no sending of data via gmail, hosting on any cloud service not in Australia (including backups) etc
Must delete data (including backups) with 3 months of gaining access
After this 3 months they are required to prove data fully deleted – this may require an inspection by suitably skilled agency

Any breach means no data access for at least 10 years and a fine of 10% of the organisations GROSS turnover.

80% of all fines to be paid the individual record holder.

f/ Every data access to be notified to the record holder via email / sms / mygov or other method nominated by the record holder, as well as being logged within the record.

g/ Any person or entity who passes on to any 3rd party for any reason not immediate health care to permanently lose access & be fined 20% of their gross income from all sources.

h/ Any attempt to water down / remove the above security features / functions to result in the instant dismissal of any politician, public servant or department employee. Any person so dismissed to be ineligible to hold any form of public office or government employment at any level for at least 10 years.