

## Submission No.48

# Inquiry into Cybersafety for Senior Australians

**City Clinic**  
**50 King Street**  
**Sydney NSW 2000**

### **Misuse of “authorised access” to personally identifying information can effect everybody.**

Currently there is no law by which Police can charge persons, who have been provided access to a computer or computer system to perform their job description, if they steal the information they have been given access to.

Any disgruntled employee, sub-contractor or other persons who have been provided access to premises can steal personally identifying information with total immunity from prosecution.

Example “Medical Practice”:

- An unethical healthcare professional or disgruntled employee uses access to patient records, provided as part of their job function, to steal the patient database.
- Patient databases have more identifying information than even most financial institutions in addition to personal medical information.
- The thief uses the information to bargain a position with a competitor or sells the information to an identity thief.
- The Privacy Policy agreed between patient and medical centre has been breached.
- The privacy commissioner requires that all effected patients be notified ASAP.
- As a result of the notification Patients become extremely nervous about their information being removed and lose confidence in the Medical Practice’s ability to keep their information safe and honour the Privacy Policy they had signed and agreed.
- The medical practice has taken many years to build its patient database and has invested \$100,000’s to build the practice
- The net result of the theft puts the medical practice into bankruptcy effecting all management, staff and creditors
- The person who has misused authorised access to steal the patient information and provide it to a competitor, start their own practice or sell it to an identity thief is rewarded and is totally immune from prosecution by Police.
- There are civil remedies however the legal costs are too prohibitive for most small businesses to even contemplate let alone action. And it takes literally years for a civil case to finalise therefore providing virtually no incentive to prosecute.

These types of thefts are occurring regularly and as a direct result of computerisation of intellectual property, customer lists, patient lists etc.

There are no laws currently available that will allow Police to charge persons involved in these type of thefts if they have been provided access. In the case of medical records, successive Governments have incentivised medical and related health practices to computerise patient records however have not provide any legislation to protect or deter thieves from stealing this information.

A recent case of theft from a Sydney CBD Medical Centre had losses and damages valued at over \$2,000,000.00. Apart from the breach of privacy for patients it left the Medical Practice financially devastated and saw many employees made redundant.

If that same thief embezzled \$2,000,000.00 they would likely go to jail and have to pay back the money embezzled or have their assets sold to recover the funds. Stealing the most valuable asset of the Medical Practice (or other type of business) has no consequence in law leaving the thief with total immunity from prosecution.

See article and comments: <http://www.scmagazine.com.au/News/314180,aussie-businesses-smashed-by-insider-fraud.aspx>

Simple legislation covering “misuse of authorised access” to remove personally identifying information from a computer or computer system is all that is needed to fix this glaring hole in our justice system. It is clear legislation has not kept pace with technology.

In the US and UK these types of thefts are illegal and perpetrators can be charged by authorities. In Australia, supposedly one of the more technologically advanced countries in the world these thefts go completely under the radar. The total cost to small business is likely in the billions of dollars per year.

Contact details:

Brad Robinson  
brad@cityclinic