Data Theft Australia
Level 7, Rockcliff Chambers
50 King Street
Sydney NSW 2000

Redacted
datatheft.au@gmail.com
datatheft.com.au

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

January 1st, 2013

Submission to OAIC: Reasonable steps' to protect personal information – December 2012

By email: consultation@oaic.gov.au

To whom it may concern,

The recently introduced Enhancing Privacy Protection Bill 2012 exposes business to risk of heavy fines if an employee misuses authorised access to steal data.

Recently the Attorney General, Ms Nicola Roxon admitted, at a Canberra Press Conference, that the greatest threat to data security within Government is corrupted public servants. Recent surveys have also indicated that over 70% of data thefts, within the business community, are committed by insiders.

A meeting with senior Fraud Squad Detectives in Sydney, on Wednesday December 19, 2012 confirmed Police are powerless to charge employees who steal personally identifying data from a Medical Centre or other healthcare facility regardless of the methods used to compromise that data.

Correspondence between the writer and various ministers on both sides of Parliament, at Federal and State level, indicate there is complete ignorance of the lack of legislative powers for Police to prosecute employees who steal critical data.

Reasonable steps' to protect personal information

All the security in the world will not stop a disgruntled employee(s) from misusing authorised access to compromise personally identifying data.

A major data theft, reported to NSW Fraud Squad in 2012 (Event number E52384988) by a Sydney based Medical Centre, indicates the highest levels of security were provided over personally identifying information of patients. No employed healthcare professional had any access whatsoever to information that would identify patients contact information apart from name and date of birth.

No staff member (reception staff responsible for data entry and management), who had access to personally identifying information of patients showed up on any audit logs as having compromised patient data.

Three Chiropractors, a Podiatrist and the partner of one of the Chiropractors used a hacker or some other clandestine method to access thousands of patients identifying information and remove it from the medical facility without authorisation of either patients or management of the medical centre.

The data was kept on independent secured servers in a cloud based facility requiring two levels of log in security to access by healthcare professionals. And access only ever provided the name of the patient, the date of birth of the patient and the medical notes (history).

The persons concerned with the fraud had not ever seen many hundreds of the patients whose information was compromised dispelling the argument they may have collected patient data directly from patients over a period of time.

As a direct consequence of the fraud the medical facility owners breached privacy with its patients, had to close down one of its sports injury centres in Sydney, lay off very experienced staff and put the centre into liquidation.

Under the guidelines of the OAIC patients were notified of the breach within one hour of it becoming known to management of the Medical Facility. For the week following the breach Medical Centre reception staff fielded hundreds of abusive calls from patients enquiring how their information could have been compromised.

Continuing SMS and email communications with patients, by the persons who removed the data without authority, continue to cause medical centre front office staff to have to deal with complaints.

Police and APHRA treated this incident as a “Commercial Dispute” despite clear evidence of fraud and extensive contractual breaches by the persons concerned with the fraud.

As this was a major breach, under the Enhancing Privacy Protection Bill 2012, the Medical Centre owners could be heavily fined yet the persons who committed the breach are immune from prosecution.

We do hope OAIC will undertake to close this significant gap in current law.

Kind regards

Redacted

Brad Robinson
Data Theft Australia
Redacted
Redacted