CHRIS MARIANI
Director, Medical &
General Risk Solutions

P: 0419 017 011

E: chris@mgrs.com.au

Authorised Representative
No.434578

MGR
MEDICAL AND GENERAL RISK SOLUTIONS

All types of fraud

Fraud can take many forms in a medical practice. Practitioners, owners and managers need to be vigilant – and put in place risk management strategies to minimise the chances of fraud occurring - and if it does, then to have appropriate insurance in place.

Recently a client contacted us to advise their employed receptionist had for numerous months been defrauding them. The employee was:

1. receipting cash payment consults and issuing receipts out of the medical records software; then
2. immediately pocketing the cash and reversing the payment - so that the daily banking amount balanced with cash receipted.

Left undetected and with the employee taking advantage of lax (or no) controls, the employee grew bolder and increased their fraud efforts to other areas they could see 'management' were not vigilant. These sorts of fraud risks can - and do - amount to tens or hundreds of thousands of dollars. While this scenario can be insured (usually under the 'crime' section of a Management Liability policy and with some insurers, under a 'Cyber/ Privacy' policy for Social Engineering, Phishing and Cyber fraud), putting in place management processes to prevent these from occurring in the first place is equally as important.

TIPS TO PREVENT THIS SCENARIO:

- The practice manager should be requesting each doctor in the practice to 'sign-off' their billings on a daily or weekly basis and give the doctor the ability to report missing transactions.
- Establish a formal process to review the right reports. For example, the 'reversal' report from the medical records system would have identified the employee who was continuously reversing transactions (a sure sign of either further training required, or fraud).
- Consider employment hiring processes, criminal history checks etc. (it was later discovered the employee had a criminal history and issues with previous employers which should have come to light before a job offer was even made)

WHAT SHOULD PRACTICE OWNERS AND MANAGER DO TO PREVENT FRAUD?

As you can see from the few examples in this article, the risks of fraud are many. Being aware and vigilant is the first step, followed by putting in place controls such as:

- separating duties so no staff member can do everything;
- create dual authorities:
  - on all payments over say $1,000,
  - cto set up new 'vendors' in your internet banking/ accounting software;
- consider what things you will do or approve yourself versus what you delegate (and delegate does not mean abdicate);
- develop management reports such as the 'reversal report';

THE EXAMPLES ON THE LEFT PAGE ARE JUST ONE OF MANY WAYS A MEDICAL PRACTICE CAN FIND ITSELF THE VICTIM OF FRAUD. SOME OF THE STRANGER CASES WE HAVE WITNESSED INCLUDE:

The employee who stole patients' credit card details (while they were undergoing a procedure) to fund their lavish lifestyle (not only did this create the fraud issue, but exposed the practice to a privacy breach under the 'Notifiable Data Breach Scheme' which came into force 22 February 2018)

The practice manager paying some of their own personal expenses using company funds as they had unfettered access to the banking and there were no controls in place such as dual authorities/separation of duties - to create and approve payments.

The business whose accounting software passwords were hacked and criminals managed to change BSB and account numbers so that when the business paid legitimate payments, the funds were transferred overseas. (please check if your accounting software can allow 'multi-factor authentication' which would have prevented this).

The employee who created a new provider number (unbeknown to the doctor), recorded their own bank account number and then swiped Medicare cards of patients, their own and family members.

The fake email from the CEO to the finance manager requesting an urgent payment to "x" for "$y". The finance manager pays as requested (the email address looked the same on first glance but was slightly different). Please ensure you verify all payments, even if this means you pick up the phone and call.

The irony is even those that should know better – get caught out. DUAL Insurance is one of the largest insurers of Management Liability in Australia. They grew rapidly from a small to a large "Lloyds underwriting agency", failing to put in place fraud controls and as a result had a claims manager defraud them of $17 million - by setting up a fake law firm and paying claims into this. This is eerily like many medical practices – where on establishment - the doctor signs off on every payment, knows what's in the bank, and has a tight control of income and expenses. They then get busy, take their eye off the accounts and delegate this to staff without putting in place any fraud controls. You can read a statement from the CEO of DUAL here https://www.insuranceandrisk.com.au/lessons-learnt-from-a-17m-fraud/

According to KPMG's January 2017 Fraud Barometer[1] the most common perpetrators are business 'insiders', with 36 percent of frauds attributable to company management and 40 percent of frauds in Australia take place over a five-year period before being discovered. 22 percent of frauds used technology – including credit card fraud; hacking into financial systems; use of fake adverts; creation of regular electronic transfers; and the use of online betting accounts to launder money.

1. https://home.kpmg.com/au/en/home/media/press-releases/2017/01/surge-fraud-i-aus-fraud-barometer-25-jan-2017.html

- make it obvious to staff you are looking – if they think you are top of the risks, they are less likely to be tempted;
- ask your accountant for their advice on what other steps you can do to manage the risks of fraud and get them to review and benchmark your expenses and income to their other medical practice clients;
- particularly where you have 'associate' doctors, give them their billings and other reports and ask they check and review for any errors, omissions, etc
- run criminal history and background checks when hiring;
- consider bringing in expert consultants to do an audit on your Medicare billings, private health; and
- purchase the right insurances including Management Liability and Cyber/Privacy Insurances and make sure you understand insurers have an expectation on areas like separation of duties, dual controls, verifying invoices.