aisma

Guide to ...

Preventing fraud in medical practices

October 2016

The rate of fraud in medical practices is on the increase. Online fraudsters are ripping practices off with phishing and ransomware scams. Unscrupulous tricksters are sending fake invoices demanding payments to non-existent companies. And there are practices whose internal financial controls are so poor they are leaving themselves open to financial loss through insider fraud. This guide, prepared by members of the **Association of Independent Specialist Medical Accountants**, offers tips and advice on reducing the risk of your practice suffering a big financial hit through fraud.

AISMA Guide to... Preventing fraud in medical practices

Insider fraud

While the vast majority of practice managers and staff working in medical practices are carrying out their roles with the greatest commitment and integrity, there is a small minority of insiders who will commit fraud if the opportunity arises. Thankfully rare, these cases when they arise can cause financial loss on a catastrophic scale.

People who commit fraud inside a medical practice could range from sophisticated criminals who target practices with poor financial controls, to staff members who are trusted by the partners but have personal financial issues or cash flow pressures.

Whatever the case, opportunities to commit fraud within the practice, for example by creating fictitious payees, syphoning off over the counter cash or de-frauding the NHS by, for example manipulating claims, adding ghost patients to increase the list size or mismanaging prescription claims, need to be minimised.

Funds generated in this way could be diverted into the hands of the fraudster without the partners' knowledge. This could also lead to a visit from the NHS Fraud Investigation team and action potentially being taken against the partners who had no knowledge of what was being perpetrated.

All medical practices should have a proper system of financial checks and balances in place to ensure the practice is not losing money through fraud.

The accountant's role

While accountants prepare the annual financial statements for the practice they do not audit the accounts and underlying books and records. Consequently, it is essential to understand that the work they do is not specifically intended to spot a fraud. Robust internal financial controls are essential.

Rate your practice controls

Start by answering the following five questions to help rate the financial controls in your practice:

1 Are the accounting records for the practice overseen by more than one person?

2 Are periodic financial reports produced monthly or quarterly and reviewed by at least one partner?

3 Is any comparison made between results from previous years and/or previous months and are discrepancies followed up?

4 Is there a designated finance partner and, if so, do they have a clear understanding of the practice's financial systems?

5 Are the people who open the post distinct from those who look after the day-to-day finances?

If the answer to one or more of these questions is 'no', the practice is at risk of fraud.

Share the burden

AISMA accountants are finding that partners in GP practices often take little

active involvement in the practice's financial affairs. Even if there is a designated finance partner, their time is eroding rapidly and they frequently rely on their practice managers to look after most aspects of the practice's finances.

But the burden of total financial responsibility for GP practices should never rest solely with the practice manager. Given the role's already wide-ranging remit, this is an unreasonable expectation.

Segregation of duties is essential.

"Busy doctors under severe time pressure must resist the temptation to hand over responsibility for their business finances to a single member of staff and simply let them get on with it. It simply is not fair to expect one person to shoulder sole financial responsibility for the practice."

Insider fraud: how it can happen

The following example highlights how poor internal controls exposed a practice to considerable financial loss.

The practice manager had been working at the surgery for many years and was a trusted member of staff with immense control over day-to-day finances. This is what happened:

Cheques for high value personal items were signed unwittingly by GP partners who did not ask to see supporting documentation.

Suppliers including HMRC and the NHS Pensions Authority were not paid on time, partly because the cash flow was in such a poor state after the practice manager's personal spending spree. The partners were unaware of the situation because the post was opened by the practice manager who shredded statements and chasers for payments.

Payroll included additional payments passed through over and above normal salary levels. There was no requirement to authorise or even show the payroll reports to the GP partners prior to instructing the bank to make the payments.

Financial reports were non-existent and the partners did not review practice results regularly. This left the practice manager free to defraud the practice over several months before the truth came to light.

Financial control check list

Use this check list to put specific financial controls in place to help reduce the risk of fraud in your practice:

- If payments are made electronically, for example by BACS transfer, supporting documentation should be presented to the partners and reviewed for reasonableness. The BACS forms should be signed as approved to provide evidence that authorisation stems from the partner group.
- Only partners should have the power to authorise standing orders and direct debits.
- A critical review of payroll reports should be carried out by someone other than the person who processed the payroll. This is likely to be a partner.
- A partner should check the practice bank statements and seek out supporting evidence for any unusual transactions. The partner should also examine the bank reconciliation each month to look out for old outstanding items.

- There should be a minimum of two cheque signatories of which at least one should be a named partner.
- When cheques are presented for signature, supporting documentation should be reviewed to ensure payments are for bona fide expenses.
- Never sign a blank cheque.
- Decide on a level, say £750, above which orders should be authorised (and evidenced as such) by a partner. For example orders for office supplies, drugs and medical supplies.
- Ensure that when deliveries are made to the practice for drugs, stationery, equipment and so on, the condition and quantity of the goods is checked before signing any delivery notes.

Safeguard cash too

Safeguards should be in place for recording, accounting for and receiving all cash coming into the practice. This is particularly relevant to dispensing practices because the increased amount of cash flowing through the practice makes it easier for someone to take unrecorded money out of the practice.

Here are some guidelines:

- Where the practice receives money from patients over the counter, a carbonised receipt book with pre-numbered pages or a sheet counter-signed by the patient should enable a quick comparison between cash recorded and physically counted. Clearly, these figures should be the same. Any discrepancies should be followed up immediately.
- Prescription cash collected from patients should equal the charges deducted by NHS Prescription Services (previously known as the PPA). While it can be difficult to match this exactly because of the delay in getting statements from NHS Prescription Services, and because sometimes charges will be deducted if an exemption hasn't been correctly claimed, large deficits should be investigated.
- Segregate tasks so that the person who handles the cash is different from the person recording it.
- Large quantities of cash should never be kept on site and should be banked regularly. This is important, both from a security point of view and from the point of view of practice cash flow.
- Restrict access to petty cash to achieve tighter control over expenditure and aid reconciliation between the petty cash records with money physically available.
- Consider installing a card machine at reception which would limit the opportunity for cash to go astray or to fall into the wrong hands.

Professional risk

Strong internal controls not only reduce the risk of financial loss but also professional risk. For example, the use of locums is commonplace but controls over their identity, qualifications and defence cover arrangements must be effective. Take these steps to protect your practice:

- Contact the GMC to check the registration of the locum and their eligibility to practice.
- Request and take a photocopy of the locum's current professional indemnity insurance cover. Without this in the event of a claim or action by a patient, the partners could be liable for the cost of a legal case.

- When the locum presents their invoice, check both the sessions you are paying for and the rates of pay. There have been cases where additional hours have been added on to the invoices and rates of pay are not as agreed.

Invoice and CEO fraud

The number of practices receiving fake invoices is on the increase. Two typical approaches of the invoice fraudster follow below, together with an example of CEO or 'bogus boss' fraud:

Fake invoice 1

An invoice arrives at the practice from a company calling itself ABC Office Supplies. The invoice looks genuine although the contact number goes to an answerphone and the address is a serviced address. The fraudster relies on the practice failing to verify the invoice against a list of known suppliers and simply paying it without carrying out any checks.

Fake invoice 2

A practice receives a letter from a company it deals with regularly for medical supplies. The letter, which appears to be on authentic headed paper, advises the practice that the company has changed its bank account and quotes a new sort code and account number for all future payments. The practice amends the payment records held with their bank. When the company sends its next monthly invoice for medical supplies received, the practice arranges a bank transfer to the new account controlled by the fraudster. The fraud is only discovered when the company chases for non-payment. There is minimal possibility of retrieving the money paid out.

CEO fraud

A member of staff responsible for making payments within the practice receives an email which appears to come from a practice partner, instructing them to make a payment using online banking. The email mentions that the payment is urgent and confidential and therefore must not be discussed with anyone else. The member of staff making the payment doesn't realize that the partner's email account has been hacked or spoofed and the request is fraudulent.

Protect your practice against invoice and CEO fraud

- Review processes for sending and receiving payments and ensure there are strong independent authentication measures in place.
- Confirm any requests to change payment details with the supplier by calling them via their verified company switchboard number.

Online fraud

According to Lloyds Bank, there has been a significant increase in many kinds of online fraud with criminals finding different ways to dupe customers into divulging their online credentials. Fraudsters see it as a low risk way of getting away with stealing money.

Malware via phishing emails remains the most common method of attack.

Phishing

Phishing scams are used by fraudsters to target medical practices by email with the aim being to steal money or acquire sensitive information. Other methods used by fraudsters include targeting medical practices using a phone scam (known

as vishing) or by text message (known as smishing).

In 2015 Action Fraud, the UK national fraud and cybercrime reporting centre, reported 8,000 reports of phishing scams every month*.

Usernames, passwords and credit card details are acquired by duping victims into clicking on links or divulging the details by phone or text.

Malware (malicious software) may also become installed onto a victim's computer and this trawls files or monitors activity for the passwords and sensitive information the fraudsters need to access bank and credit card accounts or personal files. Malware usually infects a computer when the unsuspecting user clicks on an unknown link that contains a virus.

Fraudsters are constantly developing new types of online scams. Writing in AISMA Doctor Newsline**, Ian Crompton, UK head of healthcare banking services, SME Banking, Lloyds Bank, described two relatively recent types of fraud seen targeting medical practices; ransomware and cyber extortion:

Ransomware

This is a type of malicious software, known as malware, which blocks or restricts access to the infected computer system. Fraudsters usually infect a victim's PC by encrypting files on the system's hard drive and then threatening that the user will not be able to access their data again unless a ransom is paid. The files will be almost impossible to decrypt without paying the ransom for the encryption key and this forces many victims into paying the ransom to the fraudster, usually in bitcoins which are difficult to trace.

Cyber extortion

This is a crime which occurs when a fraudster issues a threat and demand via online methods to a potential victim. As with ransomware, the demand is usually aimed at forcing a payment to the fraudster in bitcoins or they will carry out their threat. Threats can vary but may include fraudsters leaking confidential data obtained from the victim's PC out on to the Internet, or they could threaten to post thousands of negative comments about the victim's business using online review sites, causing reputational damage.

GP practices should protect themselves against these types of fraud by:

- Ensuring they have a good quality anti-virus software suite, which is scanned and updated regularly
- Carrying out operating system updates as soon as they become available
- Promoting awareness amongst practice staff to ensure they think before they click on unknown links
- Considering where their data resides. Ransomware is usually restricted to local hard drives or locally available shared drives. Information assets should therefore be held in at least two totally separated locations, such as a portable hard disk for daily backups of important data, and an additional network-attached storage for larger backups
- Retaining the original cyber extortion emails, with headers. Maintain a timeline of the attack, recording all times, type and content of the contact and report it to Action Fraud.

Lloyds Bank recommends that all fraud targeting your medical practice, even if it has been prevented, should be reported to your bank and www.actionfraud.police.uk For more information and to download

ESSENTIAL TIPS for you and your staff

- Never divulge online banking passwords or online banking secure codes to anyone on the telephone, even if you think you are talking to the bank
- Do not rely on your phone's caller display to identify a caller. Fraudsters can make your phone's incoming display show a genuine number
- Be aware that a bank will never call you and tell you to transfer your money to a 'safe' account. If you see unusual screens or pop-up boxes when using your online banking or unusual requests to enter bank passwords, log out immediately and call your bank
- There are many fake HMRC "refund" emails being sent to GPs. Do not follow the links or requests for bank details in these emails. If your accountant has not advised you of a tax refund it is highly likely to be a fraud. If in doubt, speak to your accountant.
- If possible, set up your online banking so that two separate people are required to make any payments

the Lloyds Bank online fraud guidance brochure visit **http://bit.ly/295p6Lw**

Conclusion

Clearly it will never be possible to remove all the opportunities for determined fraudsters to target your practice. There are, however, some sensible housekeeping precautions to help you protect the practice from financial loss caused by fraud or even through simple human fallibility.

They include regularly changing computer passwords for accessing the accounts system. This is especially important when members of staff or even partners leave. Take at least two types of data backups regularly and store them securely. Make sure the finance partner has an overview of how to operate, back-up and restore the accounting system.

Include in your staff handbook the policy on managing and preventing fraud in the practice.

Putting these measures in place could make a substantial difference to the financial wellbeing and overall profitability and efficiency of your practice.

For more information, support and advice on preventing fraud in your medical practice contact your nearest AISMA accountant.
Visit **www.aisma.org.uk**

** http://bit.ly/1XxoPj8*
*** AISMA Doctor Newsline, Issue 34, Summer 2016*