COUNTER FRAUD GUIDANCE FOR GP SURGERIES

Introduction

The NHSCFA has estimated that the NHS is susceptible to £91 million worth of General Practice fraud each year.

General Practice fraud relates to the manipulation of income streams or activities that breach contractual terms effected by either practitioners or staff members. Up to 60% of GP practice income is derived from payments which allocate resources according to relative workload associated with each practice.

This guidance document will take you through some of the unique risks faced by GP surgeries, as well as some of the most common fraud trends which you should look out for. At the end of this booklet, you'll find some handy tips and checklist you can use to fraud proof your own practice.

What is fraud?

Fraud is a criminal offence. In order for an offence of fraud to be proven, specific criteria need to be met.

Firstly, the person (or people) committing the offence need to have behaved in a **dishonest** manner with the deliberate **intention** of **misleading** someone else.

This needs to have been done with the aim of **making a gain** for themselves or another, or to cause the victim **to experience a loss or risk of a loss**.

There are three specific fraud offences that are frequently reported to the local counter fraud team:

Fraud by false representation - the offender commits this offence by making a false representation (lying). For example, if a contractor deliberately inflates the cost of building supplies on an invoice, this would be a false representation. Other examples would be if a job applicant filled in an application form claiming that they held a particular qualification

which they don't possess or an individual submits mileage expenses claims for journeys they did not undertake.

Fraud by failing to disclose - this offence applies where somebody fails to disclose information which they are legally expected to disclose. A good example of this is the section of a job application form where the applicant is asked to share any existing convictions or pending charges or an employee fails to disclose a change in their right to work.

Fraud by abuse of position - this offence refers to occasions where a person is in a trusted job role which gives them access to something valuable or computer systems with approver access. That could be access to a bank account, authority for making decisions about which contractors are awarded NHS contracts, access to computer systems containing patient data or access to approve timesheets. If a person abuses this access for their own personal gain they may be prosecuted for fraud by abuse of position.

Fraud offences carry a maximum sentence of **10 years in prison** and the potential to face an **unlimited fine.**

How does fraud occur?

Fraud often occurs due to a weakness in controls, which creates an opportunity to commit fraud. Fraud may occur due to the following;

- Lack of verification process
- Failure to follow procedures
- Poor record keeping
- Lack of supervision
- Lack of fraud awareness
- Lack of segregation of duties
- Lack of data sharing

Who commits NHS Fraud?

NHS Fraud comes in many different forms, and can be committed by several different groups. **Patients** may adopt an alias in order to obtain additional medication, **contractors** may inflate costs or deliberately submit duplicate invoices, **organised criminals** may target NHS accounts teams, and unfortunately, a very small minority of **NHS staff** will attempt to defraud their employer.

The main GP fraud types are:

- **False claims** by general practices for allowances, reimbursements, expenses or grants which are not related to patient care.
- Unlawful **prescribing** by general practices. For example, prescribing to patients who do not exist, are deceased or self -prescribing.
- Deliberate **misrepresentation** of patient list size and/or demographics by health care service providers in order to attract higher funding. For example, older patients who attract higher funding not being removed from the practice list when they are deceased or fictitious patients being created to attach higher funding. (**Capitation figures**)
- **Diversion of global sum -** This relates to core funding payments made to general practices for essential and additional patient services which are not used for their intended purpose.
- **Diversion of funds -** This relates to general practice funds being diverted or stolen by a practice manager or employee (this includes pension contributions).
- **Conflicts of Interest** - Where a general practitioner's decision making in respect of commissioning is suspected to be influenced or impaired by a personal interest, role or relationship. For example, where they misuse their position to further their own interests or those close to them, in order to obtain a financial gain or another type of benefit or advantage
- **Inducements-** This relates to a general practitioner asking for or accepting an inducement, gift or hospitality to influence decisions about registering, prescribing, treating or referring patients or commissioning services for patients.
- **Disposal of NHS drugs -** This relates to the improper disposal of NHS drugs without authorisation or for personal gain. This includes the selling and donation of drugs or exporting of drugs overseas.
- **GP practice employees -** This relates to the activities of employees at a GP practice. This can include false expenses or overtime claims, misappropriation of petty cash float, working whilst on sick leave or other leave, failing to disclose conflicts of interests.

How are GP surgeries affected?

Prescription Fraud

There are numerous ways in which you could be targeted by prescription fraud.
The simplest way for someone to commit this offence is to **steal** an unattended prescription pad. ** ELFT's Primary Care Directorate (PCD) have their own Standard Operating Model on the management of prescriptions in Primary Care. Please refer to

ELFT's 'Primary Care Services – Prescription Security Protocol' for guidance on how to manage lost or stolen FP10 prescription pads. ** (Click on the icon for the protocol)

Prescription
Security Protocol - P

Another area of risk comes from the ability of staff to **reprint prescriptions**. It is best practice to ensure that the ability to reprint prescriptions is only provided to appropriate staff.
Scripts can also be forged by fraudsters, eg, changes can be made to the quantity prescribed, or drug prescribed in order to increase the quantity or to access controlled drugs. Controlled drugs are particularly liable to abuse so caution must be taken at all times.
You may come across patients who repeatedly claim that they have **lost their prescription**, or who use out-of-hours services to bypass safety measures at your practice.
Vulnerable patients can be **exploited** by family members, who could contact out-of-hours services to request a new prescription is issued on behalf of their relative.

Prescription Fraud Case Studies

- Junior receptionist who did not have the ability to reprint prescriptions
- Waited until colleagues left the their work computers unattended
- Issued 43 scripts for Zapain and Diazepam over 2 years
- Found guilty of committing Fraud by Abuse of Position
- Sentenced to 18 months in prison, 150 hours unpaid work and rehabilitation

- A doctor forged over 400 prescriptions in the names of three of his patients and obtained medicines to treat himself for depression using these names
- In total, the doctor forged 243 prescriptions in the name of one of his male patients, 173 in the name of the another and 24 using the third patient's identity
- The total value lost to the NHS was £10,047 and the patient details he used were all entitled to free prescriptions and did not have to pay.
- The doctor was given a four months jail sentence suspended for 12 months and ordered to pay £10,047 compensation to the NHS within a year, after he pleaded guilty to three charges of fraud.

Preferential/manipulation of use of Agency Bookings

This can occur when agency staff that are booked to work within practices, e.g. GP's, unfairly try to gain an advantage for their agency over other agencies, by recommending and trying to persuade the Practice to take on additional staff from their agency over other alternatives available to the Trust. This unfair practice can also result in the agency member of staff benefiting financially from this as they may have an arrangement in place with their agency that they receive an additional rate per hour or other payment if they influence the agency booking procedures.
Other examples can include Practice staff on part time hours agreeing with practice managers to be paid a lot more via an agency to cover other days in the same service.

Failing to declare secondary employment/business interests

This is when a member of staff is working for ELFT and has a second job or business interest elsewhere that they have failed to declare to the Trust, which is a requirement under ELFT's Standards of Business Conduct Policy. All staff are required to declare any existing outside employment/business interests on appointment to the Trust, and any new outside employment/business interests as and when they arise throughout the course of their employment with ELFT.
The Standards of Business Conduct Policy at Section 13 defines secondary employment/business interests as "Outside/additional employment means employment and other engagements, outside of formal employment arrangements. This can include directorships, non-executive roles, self-employment, consultancy work, charitable trustee roles, political roles and roles within not-for-profit organisations, paid advisory positions and paid honorariums which relate to bodies likely to do business with an organisation."
There are several reasons why "second jobs" and/or Business Interests are required to be declared. One of the reasons is that the Trust needs to ensure that the secondary employment/business interests is declared is to ensure the two do not conflict with, or be detrimental to the employee's NHS work or the work of the Trust as a whole. This is a key consideration when a Declaration of Interest Form is being reviewed by management. An example of where secondary employment/ business interest could conflict with an individual's role at ELFT is with the ordering process. E.g. Over ordering of medical equipment/other supplies and using them in other roles held outside of the Trust that they have not declared, or buying supplies from friends/family business that have not been declared. Other considerations relate to the compliance with the Working Time Directive.
To declare secondary employment/business interests, staff should complete Appendix G from the Standards of Business Conduct Policy. Click on the link below for the form.
http://elftintranet/download/6aedf6e5-47a2-48de-a2a6-752702464c32/f/Appendix_G_-_Declaration_of_Interests_Form.docx
The completed form must be sent for approval by a Service Director (in the case of secondary employment), and for business interests, to their managers, who may wish to liaise with the Director of Corporate Governance when considering the business interest. All approved forms are required to be sent to elft.declarations@nhs.net

At the end of this document you'll find a series of **checklists,** including one which will help you to consider whether you need to update or amend your current financial arrangements.

Patient Identity Fraud

Patients may register at numerous medical practices using **false details** in order to access additional medication or services.
There have also been cases in which patients who have been sent to prison have arranged for **associates** to attend their GP practices in order to secure prescriptions for controlled drugs.
Unfortunately, GP practices have little control over who registers as a patient. However, the simple act of **requesting proof of identity/address** can act as a deterrent as it shows your surgery is not an easy target.

Current Fraud Trends Affecting the Whole NHS

- Cyber enabled frauds including phishing
- Timesheet fraud
- Recruitment fraud
- Taxi fraud – booking Trust taxis for personal use, non-ELFT staff using the Trust's cost centre code to book taxis
- Prescription fraud, forged/altered prescriptions, 'ghost' patients due to multiple registrations at GP practices using false ID's to obtain several prescriptions forms (as above)
- Undeclared secondary employment
- Falsely claiming to be sick whilst abroad
- Expenses Fraud

- COVID specific scams - Staff falsely claiming to be isolating and working elsewhere, increased risk of payroll fraud, on-line scams where goods ordered are never received, Text (SMS) scams purporting to be a genuine companies to obtain individual's personal data. Many GP's are receiving fake HMRC 'refund' emails. Do not follow the links or requests for bank details in these emails

Phishing

There are many forms of phishing emails that you may encounter. The overall aim of a phishing email is to gain access to money, but they may take several different routes to do so. Phishing emails are designed to get you to do one of the following:

1. Send an **immediate payment** directly to a fraudster's bank account
2. To click on a link within the email which will take you to a **phishing website**, where your bank details, personal information, or log in credentials to genuine sites will be harvested
3. To **provide information** which will be used in another fraud later down the line (e.g. names of managers, people dealing with payments, suppliers which are being used etc.)
4. To download a **malicious attachment** which will infect your computer with malware.

A key element of phishing is that it is designed to look like it has come from a genuine source. They may impersonate a legitimate company or even another member of NHS staff. There are several tactics that are used and that you should look out for. Please see the guide at the end of this document for advice on what to look out for.

Beware of phishing emails - A reminder - common tactics used in phishing emails to be aware of:

- Slightly amended email addresses - changes can be very minor
- Spelling and grammatical errors and are often written poorly
- Use of pressure – The messages usually create a sense of urgency by claiming your account will be shut down, late fees will be applied or you may not be paid this month if you don't comply
- Use of a bait - offers of refunds, "special offers", or information about pay rises etc.

Tips

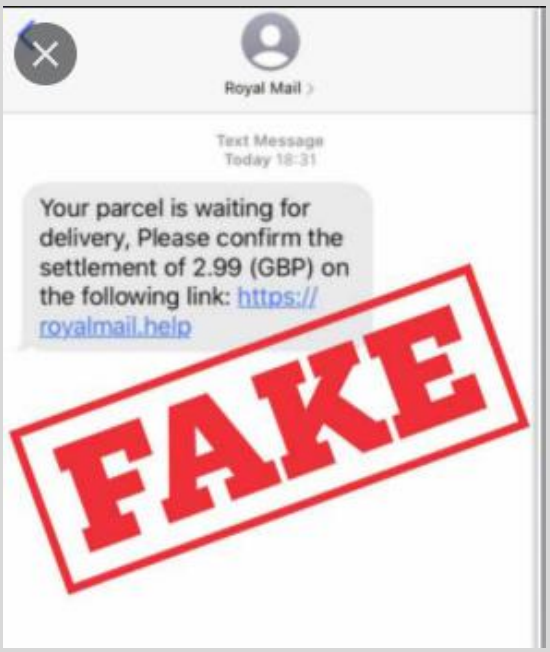
- If in doubt, do not open any attachments or files
- Look at the email address to see if it has been spoofed
- Retain the original cyber email, with headers, and forward, as an attachment to the IT Department, LCFS and to spamreports@nhs.net and then delete the email
- Promote awareness amongst practice staff to ensure they think before they click on unknown links

Phishing Case Study

Intensive Care Nurse Loses £12k of Personal Savings

An intensive care nurse was contacted via phone call after a night shift.
The call appeared to be from her bank, Halifax. The number displayed on her phone screen matched the number which was printed on the back of her bank card.
The nurse was advised fraudulent activity had been detected on her bank account, with a payment of £7,000 due to leave her ISA imminently. She was persuaded to set up a new ISA and to transfer £12,000 into that account. The "new" account actually belonged to a fraudster.
This scam was actually several days in the making. The nurse had unfortunately fallen foul of a phishing email that had been sent to her, purporting to be from British Gas. It featured their official logo and claimed she had an overdue bill which was due to become very steep as late fees were going to be added.
The nurse was directed to click on a link which would allegedly take her to the British Gas website where she could prevent the late fees from being added and resolve the overdue bill. When she clicked on the link, she was taken to a phishing website where her personal and financial details were harvested.
This gave the fraudsters everything they needed to convincingly impersonate her bank on the phone. They had used spoofing software to disguise their real number by making it look as though they were calling from Halifax customer services.
Fortunately, she has been refunded the money.

Scam Text messages



NHS employees have received scam text messages on their work and personal mobile phones, purporting to be from the courier company Hermes, Royal Mail and their banks saying that an additional payee has been added to their account and if this is not accurate could they click on the link in the text message and verify their credentials. Before you know it, you've given the fraudster your log in details, password etc to your internet banking.

THERE IS SOMETHNG YOU CAN DO ABOUT THESE SPAM TEXT MESSAGES?

7726 is a free, spam text reporting service that your mobile phone provider has set up. The Mobile network operators look at the text messages sent to them via the 7726 number and if they get enough information from that number, they will pass it on to the police. A dedicated team within the police actually receive the referrals directly from the mobile network operators and not from individual members of the public.

WHAT STEPS YOU CAN TAKE?

If you receive a spam text message, you can forward the message to 7726. You may get an automated response thanking you for your report if your mobile network provider supports this number.

If you have an Android device, you can alternatively tap the 'Report Spam' button in the messaging app. This message is displayed if it comes from someone who isn't in your contacts or if it looks suspicious to Google.

WHAT HAPPENS IF YOU DON'T RECEIVE A CONFIRMATION TEXT MESSAGE FROM 7726 OR IT STATES YOUR MESSAGE DIDN'T GET THROUGH?

In some cases people have stated that their messages were unable to get through to the number and their network didn't support the number. Therefore a workaround for this is to save the 7726 number as a 'contact' in your phone book, under a name that you will

easily remember, such as SPAM, and then forward the message to that contact which is the 7726 number.
Users should make sure that when saving the number they ensure 7726 is saved and not another variation such as +447726 as this could affect the text being sent.
Users can also block the sender and delete the message.

TOP TIP - An easy way to remember this number is that 7726 on your keypad actually spells out the word SPAM.

Mobile users should check with their mobile network providers if their network uses a variation of the 7726 number which is unique to them, but still gets through to the required team at the mobile company.

Who Investigates Fraud at your GP Practices?

The LCFS' will investigate any allegations of fraud, bribery or corruption that may occur at your Practice. You can make a referral to the Counter Fraud Team via email, by phone or via the online reporting tool found on the Intranet. This is the same method that Practice Managers and/or staff can use to make a referral. The LCFS will take the details of the allegation and any accompanying documentation during communications with the referrer.

What can you expect from ELFT's Counter Fraud Team?

1. The LCFS' are two full time members of staff, who are available to discuss any issues or provide general advice if you have a query.
2. The LCFS' can provide Counter Fraud awareness sessions for your teams to inform them of fraud in the NHS, what fraud types of fraud can occur, what your practices should look out for, provide tips and allows staff attending the session to ask questions and provide feedback.
3. The LCFS will send regular links of bite size monthly videos which they record so managers can cascade to staff.
4. The Counter Fraud Team issue their Fraud booklet called "FraudTalk". This features local and national cases, what fraud investigations the LCFS' have been involved with, any new frauds/scams that may come to the LCFS' attention by the NHSCFA, Police or other Fraud teams.
5. The LCFS will forward any Fraud Prevention Notices (FPN's) issued by the NHSCFA as and when they are issued. These will inform your practice what new frauds or risks that have been identified nationally as the ever-changing pressures of COVID take place. As part of this the LCFS may ask for input in respect of the control measures you have in place. The LCFS may also make recommendations as to what controls you should/could introduce to mitigate those risks. Similarly, if a Practice Manager identifies a new risk or adds controls to reduce a risk they may already have, they should contact the LCFS and provide the details, so the LCFS can update the Fraud Risk Assessment (FRA). The FRA is an ever changing document.

6. The provision of Counter Fraud material such as electronic posters and leaflets etc. to display in your staff areas.
7. You can also follow the Counter Fraud Team on Twitter at Fraudtalk@elft1

Think Prevention and Good Practices

Here are some tips on how to protect your practice against the risk of fraud, including how to implement financial controls.

1. Financial responsibilities should be clearly defined and shared amongst appropriate staff, such as the timely review of budget statements to ensure any signs indicative of fraud and error are identified. Keeping tight checks on financial transactions and also making comparisons between the financial results from previous years or months and following up on any discrepancies
2. Segregation of duties ensures there is oversight to identify errors and prevent fraud or theft
3. 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
4. Restrict access to petty cash to achieve tighter control over expenditure and aid reconciliation between the petty cash records with money physically available.
5. Consider installing a card machine at reception which would limit the opportunity for cash to go astray or to fall into the wrong hands.
6. Review the payroll – all managers should be checking what staff are on their payroll to identify any leavers still on the payroll, correct amendments have been made if staff change their job roles or contracted hours, to ensure they are paid the correct amount. If a member of staff leaves, change forms must be actioned on time to prevent overpayments.
7. Keep a receipt of all cash transactions
8. Liaise regularly with the Finance Department and explain importance of this, budget statements.
9. Ensure all staff are familiar with the Counter Fraud and Bribery Policy http://elftintranet/sites/common/Private/Contentobject_View.aspx?id=29290 and Standards of Business Conduct Policy, http://elftintranet/sites/common/Private/Contentobject_View.aspx?id=31183

NHS
East London
NHS Foundation Trust

Practice Checklists

Prescription Fraud Checklist
Are prescription pads securely stored and their whereabouts monitored?
Are electronic prescriptions issued wherever appropriate?
Are you happy with which members of staff are able to reprint prescriptions?
Are all staff members advised to lock their computers when they leave their desks?
Do you audit reprints of prescriptions to identify trends (e.g. the same patient is always reporting missing prescriptions, the same member of staff is always reprinting scripts for particular medications etc.)?
Do you have a process in place to flag patients who repeatedly report lost or misplaced prescriptions?
Are patients who repeatedly report lost prescriptions signposted for support or offered alternatives such as electronic prescriptions?
Are you aware of how to flag a patient's record so that if they contact out of hours numbers call takers are aware of issues such as trying to gain access to particular drugs?
Are all members of staff aware of the reporting routes for safeguarding concerns if family members are suspected of intercepting medication?

Useful Resources

NHS Counter Fraud Authority
Information about fraud and the NHS, including a reference guide on the types of fraud most commonly encountered and an anonymous reporting option. https://cfa.nhs.uk/

NHS Digital
Find NHS Digital advice on avoiding phishing emails by clicking on the link above. You can also find links to the NHS Digital campaigns on cyber security issues by clicking here. https://digital.nhs.uk/cyber-and-data-security

GOV.UK List of Proof of Identity Documents
The link above will take you to a list of proof of identity documents which are approved by the government. This list is useful to refer to when requesting new patients to provide proof of identity or address. https://www.gov.uk/government/publications/proof-of-identity-checklist/proof-of-identity-checklist

National Cyber Security Centre
Suspicious emails which are received at home can be reported to the National Cyber Security Centre. The website also provides lots of advice about staying safe online, with areas of the website dedicated to advice for keeping safe online at work and at home. https://www.ncsc.gov.uk/

Action Fraud
A national organisation providing advice on all aspects of fraud. This is a useful resource for both staff and patients, as there have been numerous scams throughout the pandemic in which NHS services (including GP surgeries) have been impersonated to defraud vulnerable people. https://www.actionfraud.police.uk/

Further Advice and Guidance

If you have any questions about this guidance, or have a concern about possible fraud, bribery or corruption, please contact ELFT's Counter Fraud Team, Zenda Butler (LCFS), on 07908 194431 or via zenda.butler@nhs.net If your concern relates to Luton and Bedfordshire Mental Health and Wellbeing Service or Bedfordshire Community, please contact LCFS Beth Raistrick on 07908 425280 or email Bethan.raistrick@nhs.net

******PLEASE NOTE BOTH LCFS' ARE WORKING FROM HOME DURING THE PANDEMIC. PLEASE CONTACT EITHER ZENDA OR BETH VIA EMAIL OR THEIR WORK MOBILE NUMBERS UNTIL FURTHER NOTICE. ******

All enquiries will be treated in the strictest of confidence.

You can also report any suspicions of fraud or attempted fraud to the NHS Counter Fraud Authority online at https://cfa.nhs.uk/reportfraud or through the NHS Fraud and Corruption Reporting Line 0800 028 4060