Counter Fraud Guidance for GP Surgeries

Version 5 - 2025

Introduction

Understandably, fraud isn't the first thing you think about when you consider a career in the health service.

Unfortunately, fraudsters do target the NHS. As a large, complex organisation opportunities may arise for unscrupulous people to try and divert money intended for patient care into their own pockets.

The NHS Counter Fraud Authority is tasked with overseeing the counter fraud approach taken by the NHS nationally. Their latest estimate puts the amount of NHS money which is vulnerable to fraud at £1.2 billion. That's the equivalent of 40,000 staff nurses or 308,000 hospital beds.

This guidance document will take you through some of the unique risks faced by GP surgeries, as well as some of the most prevalent fraud trends which you should look out for.

At the end of this booklet, you'll find some handy checklists you can use to fraud proof your own practice.

Any Questions?

If you have any questions on the contents of this guide, please don't hesitate to contact the ICB's Local Counter Fraud Specialists:

Rosie Dickinson
rosie.dickinson1@nhs.net / 07825 228 175

Steve Moss
steven.moss@nhs.net / 07717 356 707

What is Fraud?

Fraud is a criminal offence - in fact, it's the most common offence in the UK.

Fraud offences involve the victim being misled or lied to during the commission of the offence.

The perpetrator seeks to make a gain for themselves or another, or causes the victim to experience a loss (or exposes them to a risk of loss).

Types of Fraud Offence

There are three main fraud offences that are frequently reported to the ICB's Local Counter Fraud Specialists:

Fraud by False Representation - an offender lies about something in order to make a gain. For example, a cyber criminal impersonates a supplier to divert invoice payments.

Fraud by Failure to Disclose - a person fails to share information that they are legally expected to share, and they have done this to secure a gain for themselves. For example, a person does not disclose that they have a relevant criminal record when applying for an NHS role.

Fraud by Abuse of Position - this refers to occasions where a person holds a trusted position and they exploit this for their own benefit. Examples include a member of staff using their access to finance systems to divert NHS money into their own account, or a procurement manager ensuring that a friend's company gets awarded NHS contracts.

The maximum sentence for fraud offences is 10 years imprisonment. An unlimited fine can also be applied. If the person who committed a fraud offence holds a registered profession, their regulating body is notified and they may be struck off.

The Economic Crime and Corporate Transparency Act 2023 introduced a new offence - **Failure to Prevent Fraud**. Under this legislation, large organisations can be prosecuted if an "associated person" (staff, supplier, contractor) commits fraud in a way that benefits the organisation - if it is found that there were insufficient fraud prevention measures in place.

Why does fraud occur?

In the 1950s, Criminologist Donald Cressey developed a theory of how fraud takes place. He suggested that three factors needed to be present for fraud to take place:

- **Opportunity** - a process or system is open to manipulation or abuse.
- **Pressure** - the individual has a drive to commit the offence. This could be due to issues such as addiction, personal debts, or to fund a particular lifestyle they feel entitled to.
- **Rationalisation** - the person is able to justify their actions to themselves.

When these three factors are present, the risk of fraud occurring is high.

What does this mean for your practice?

Arguably, you have the most control over the **opportunity** section of the fraud triangle. By reading this guidance you should be able to check your surgery for areas of opportunity that could be exploited. There are checklists at the end of the document which will help to create an action plan to improve your fraud proofing.

It is important to remain mindful of the role of **pressure**. If a patient is repeatedly claiming to have lost their prescription, it could be a sign of a safeguarding issue such as substance addiction or pressure from a family member or criminal group.

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 who target NHS staff, systems, and premises.

Unfortunately, a very small minority of **NHS staff** may attempt to defraud their employer.

How are GP surgeries affected?

Prescription Fraud

The simplest way for someone to commit this offence is to steal an unattended prescription pad.

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.

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 may contact out-of-hours services to request that a new prescription is issued on behalf of their relative.

Case Study - Lisa Rowles

Lisa was a junior receptionist with no ability to reprint prescriptions. She waited until her colleagues left their computers unattended.

She used their accounts to reprint 43 scripts for Zapain and Diazepam over a 2 year period.

She was found guilty of Fraud by Abuse of Position and was sentenced to 18 months in prison, 150 hours unpaid work and rehabillitation.

Case Study - Ashleen Murray

Ashleen stole a prescription pad during an appointment with her GP.

She forged signatures on 22 prescriptions, which she handed in at pharmacies covering a wide geographical area.

She was found guilty of Fraud by False Representation and was sentenced to 240 hours of unpaid work and 60 days of rehabilitation.

Patient Identity Fraud

Patients may register at numerous medical practices using false details in order to access additional medication or services. There have been local cases where patients who are in prison have sent associates to their GP practices to collect prescriptions for controlled drugs.

Please remember that GP practices cannot refuse to register a patient simply because they have no proof of address or identity documentation.

The CQC have released advice on supporting people who are homeless to access primary care and further advice can be sought from various organisations (e.g. Shelter, Refuge, Citizen's Advice and NHS England). However, the simple act of requesting proof of ID / address can act as a deterrent to those with dishonest intentions.

Practice Funds

Practice funds are always going to be of interest for fraudsters. They may be targeted by those outside of the organisation, such as unscrupulous contractors or organised criminals.

Unfortunately, practice funds can also be misappropriated by surgery staff. Although this is rare, whenever it does happen it tends to be picked up by the press. A quick search on Google brings up numerous articles relating to high profile examples of where this has happened.

When practice funds are targeted, the impact can be devastating. 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.

Case Study - Karen Evans

Karen was employed as a practice manager at a GP surgery in Manchester. Within a month of starting her role, she had started to siphon off practice funds.

The fraud was first detected when the partners had to arrange a bank overdraft of £25,000 as they did not have enough money to pay their staff.

An internal investigation discovered that Karen had moved £600,000 into her own bank accounts.

The money Karen had taken had been spent on gambling websites. At one point, she won £120,000 but lost all of it within days. It emerged that she had previously defrauded a different GP practice of £77,000.

As a result of Karen's actions, 4 of the 5 GPs at the practice had to step down or take early retirement. Karen was sentenced to 3 years and 4 months in prison.

Job Applicant Identity / Qualification Fraud

The pre-employment checks process can feel long winded, but it is absolutely vital to ensuring the safety of your staff and patients. It is always worth reminding any staff who deal with recruitment of the real reason why these checks are so important.

Pre-employment checks are designed to verify the identity of the applicant, ensure their qualifications are genuine and valid, and to establish whether there are any criminal convictions / pending charges that could have an impact on the safety of your practice.

During the Covid-19 pandemic, the process of checking identity documents and qualifications changed. Many of the changes have been continued, and NHS Employers have extensive guidance on their website to walk you through every stage of the process.

It may surprise you to learn that it's possible to buy fake qualifications from eBay, where they are listed as a "novelty item". There are also some shocking stories out there about people who have failed to disclose relevant criminal history when applying for NHS roles (for example, Craig Alexander, who failed to mention his conviction for armed robbery when he successfully applied for a role at NHS Brent).

Case Study - Zholia Alemi

Zholia Alemi was employed in the NHS as a Consultant Psychiatrist for around 22 years. Originally from New Zealand, she came to the UK in the 1990s as part of an international recruitment drive to fill NHS roles.

Zholia worked with vulnerable patients, and held roles at various NHS organisations all across the country.

She first came to the attention of the police when she attempted to alter the will of one of her patients, an 87 year old lady who had dementia. Within 4 months of meeting the lady at a dementia clinic, Zholia had made an application for power of attorney and attempted to change her will so that the lady's £1.3 million estate would be left to her.

During the police investigation, they uncovered that Zholia had never passed her first year of medical training. When she arrived in the UK, Zholia had produced a fake certificate which she had presented in order to "prove" that she was properly qualified. Unfortunately, the legitimacy of this certificate was not checked and Zholia began her NHS career.

She was sentenced to 5 years in prison for her attempt to alter the will of her patient. In addition, she was later charged with 13 offences against the NHS. This includes multiple counts of fraud by false representation, as well as a charge of making a false instrument which relates to the fake qualification certificate.

Zholia did not hold the right qualifications for the role she was carrying out for the NHS. In 2023 she was sentenced to a further 7 year prison sentence for fraud offences against the NHS.

Cyber Enabled Fraud

As technology plays a huge role in modern life, it is perhaps unsurprising to hear that 80% of reports to Action Fraud relate to cyber-enabled fraud. Cyber-enabled fraud is where the perpetrator has used technology to facilitate their offending.

Cyber enabled fraud takes many forms and fraudsters are becoming ever more sophisticated. Many use artificial intelligence (AI) to create high quality fraudulent materials.

Phishing Emails

Phishing emails are often the first step in a cyber-fraud attack. They may aim to steal your log in details, persuade you to make unnecessary payments, divert genuine payments, gather information for use in fraud, or to spread malware and viruses onto your device.

These emails are designed to look like they've come from someone you know or trust. Tactics used include claiming there is a problem with your payroll or email account, or asking you to access a "secure file sharing site". These emails contain links which, when clicked, take you onto convincing fake websites where you are asked to "log in". The fraudster is then able to capture your login information and access your accounts.

Potential warning signs of phishing

- Lack of personal greeting
- Unexpected links or attachments
- Hidden links
- Sender's email address has changed
- Missing contact information
- Sender is putting pressure on you
- Unusual requests
- Use of fake deadlines to panic you

Case Study - Nurse Loses £12k in Phishing Scam

An intensive care nurse received a phone call after finishing a night shift. The call looked to be from her bank, Halifax. The number on her screen matched their customer services number.

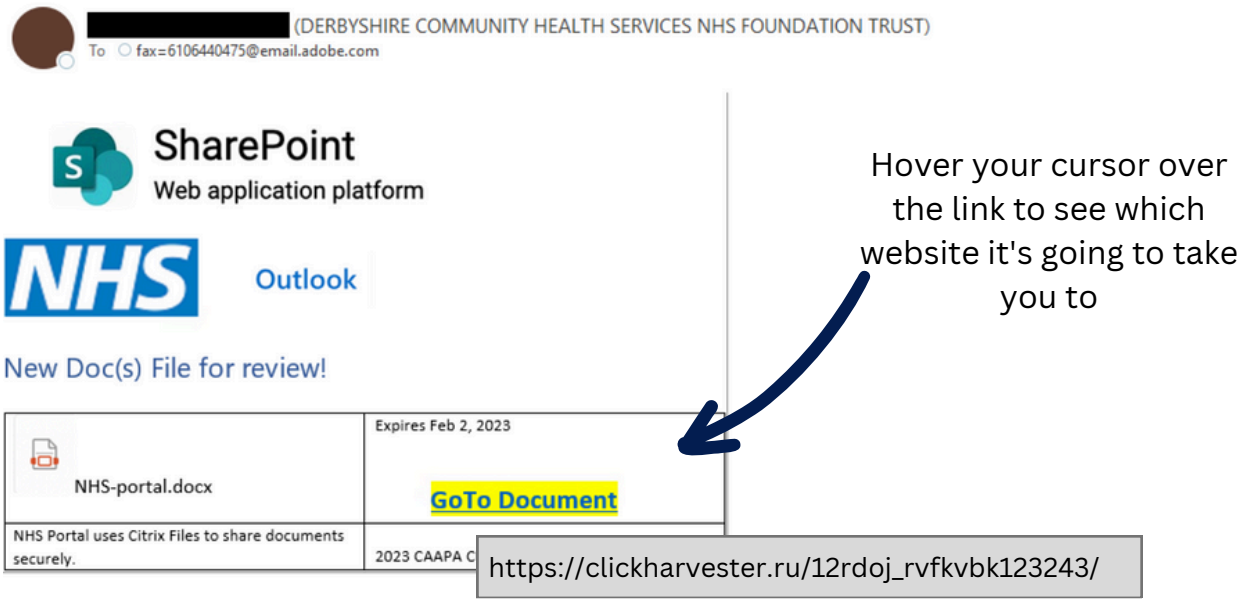
The nurse was told that her bank account had been compromised, and that scammers were trying to take £7k from her ISA. The caller said that to protect her money she needed to empty her ISA into a new "safe" account. She moved her entire £12k of savings, but sadly the safe account belonged to a fraudster.

Earlier that week, the nurse had interacted with a phishing email designed to look like it had come from British Gas. The fraudsters had directed her onto a phishing website which they used to gather information about the victim, including her name, address, and which bank she was with.

This gave them everything they needed to impersonate her bank over the phone. They even used spoofing software to disguise their phone number, pasting the bank's contact number over their own. Luckily, she has since been refunded.

Phishing Advice

- Pay close attention to sender's details.
- Never click on unexpected links and attachments.
- Watch out for emails that are trying to pressure you or panic you into acting quickly.
- You can hover over hyper links to see where they will take you (please see below).
- If you think you have clicked on a dodgy link or attachment, notify your IT provider as soon as possible.



Office Supply Scams

Office Supply Scams have been spotted at GP surgeries across the UK. Practices are contacted by an "office supply company" regarding an outstanding invoice which is likely to sit just below the £1000 mark. Items billed for have included printer ink, toners, and generic supplies such as gloves and facemasks.

Often, the person sending the invoice will state that the goods were ordered by a previous employee. These scams sometimes take place in the first few months after a new practice manager has been appointed. In these examples, the fraudster will claim it was the previous practice manager who placed the order.

The office supply company can be very aggressive in chasing payment. They may appear on Companies House, but usually do not have much of an online footprint - e.g. no website where orders would be placed.

In some cases, the fake companies have sent unwanted items or empty boxes to GP surgeries, and then used the delivery note as "proof" that the items were ordered.

Advice

- Make sure staff are aware of this scam methodology and unexpected invoices are challenged.
- Invoices should correspond to a Purchase Order. Ask the sender to confirm the PO number.
- Put unexpected deliveries to one side. Ensure nobody uses or removes the contents.
- If you need advice or support, you can contact the ICB's Local Counter Fraud Specialist.

Mandate Fraud

Mandate Fraud is when a fraudster impersonates a genuine supplier. They request that the bank details held on file for the supplier are updated. This results in future invoice payments being sent to the wrong bank account. It is often carried out via email.

Mandate Fraud, when successful, can generate a massive pay day for the criminals. Those committing this type of fraud are therefore very determined and will go to significant lengths to create a convincing disguise. We have seen examples where fraudsters spent months monitoring a compromised NHS email account, waiting for an opportunity to act.

Scammers like to use compromised email accounts to locate useful documents and intelligence such as copy invoices, names of key staff, names of systems or processes, payment dates etc. Account compromise is often carried out using phishing emails.

Fraudsters may use hi-jacked email accounts to carry out a mandate fraud, or create spoof email accounts that look “right” at first glance. Where possible, they will lift branding and formatting from genuine email exchanges (such as copying a person's email signature, but removing phone numbers).

To avoid falling victim to a mandate fraud, it is essential that staff who deal with payments are aware of the steps that must be taken if a request to change bank details is received. You'll find a checklist to assist with this at the end of the guide.

Case Study - Mandate Fraud

In 2018, Mersey Care NHS Foundation Trust were hit by a mandate fraud.

Criminals contacted the Accounts Payable team, impersonating a genuine supplier who was used by the Trust.

The fraudster pretended to be a known contact within the supplier’s organisation.

They put in a request for their organisation’s bank details to be updated shortly before submitting a single invoice which totalled over £900,000.

Unfortunately, the invoice was paid, with the funds landing in a bank account controlled by the fraudsters.

Password Advice

- Do not recycle passwords, each account should have a strong, unique password.
- Consider using a passphrase made up from three random words, some favourite song lyrics or a line from a book or film.
- Avoid using names of family members, sports teams or pets. This information can be accessible on social media - even if your accounts are secure, friends and family may be less aware and share this information unintentionally by tagging you in their posts.
- When updating your password, come up with a completely new password instead of just changing the digit on the end.
- If you want to find out how good your password is, you can check the strength of it using the How Secure is My Password website.

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 online reporting tool.

NHS Digital

Find NHS Digital advice on avoiding phishing emails by clicking the link above. You can also find links to the NHS Digital campaigns on cyber security issues by clicking here.

NHS Employers

Guidance on relevant topics such as how to complete pre-employment checks.

GOV.UK List of Proof of Identity Documents

GOV.UK publish a list of identity documents which are approved by the government.

National Cyber Security Centre

Suspicious emails that are received by non-NHS.net email accounts can be reported to the National Cyber Security Centre. They also provide lots of advice about staying safe online.

Action Fraud

A national organisation providing advice on all aspects of fraud - this is a useful resource for patients.

Further Advice and Guidance

If you have any questions about the contents within this guidance document, you are very welcome to contact the ICB's Local Counter Fraud Specialists - Rosie Dickinson, Shaun Fleming or Steve Moss. You can reach the team using the following details:

- **Rosie Dickinson**, rosie.dickinson1@nhs.net 07825 228 175
- **Shaun Fleming,** shaunfleming@nhs.net 07484 243 063
- **Steve Moss**, steven.moss@nhs.net 07717 356 707

If you have a suspicion of fraud and you are not sure where to report it, please feel free to contact any of the team for advice and support.

Who investigates fraud at GP practices?

It can be a little bit complicated establishing who will investigate an allegation of fraud when a GP surgery has been targeted. Depending on where the financial loss has occurred, it may be investigated by Local Counter Fraud Specialists from either the ICB or NHS England, or the Police.

The interaction between GP Practices and a Local Counter Fraud Specialist (LCFS) usually arises when:

- A GP Practice contacts the ICB for advice regarding a suspicion of fraud involving **practice funds** and the matter is passed to the LCFS. In circumstances such as this, the advice is often to report the matter to the Police. However, with approval from the ICB the LCFS can provide fraud prevention guidance and support to the practice.

- The ICB has concerns about the possible misuse or abuse of **ICB funds** by a practice and the matter is passed to the LCFS for investigation. Authority to investigate is dependent on who holds the contractual and financial liability.

- NHS England has concerns about the possibility of misuse or abuse of abuse of **funds they have provided**. NHS England have their own in-house team of LCFSs and their involvement in an investigation is again dependent on who holds the contractual and financial liability.

If you are ever in doubt about who to report a concern of fraud to, please do feel free to contact Rosie, Shaun or Steve for advice and signposting. Please see the previous page for our contact details.

About Audit Yorkshire

The ICB's counter fraud and internal audit service is provided by Audit Yorkshire.

Audit Yorkshire is an NHS internal audit, local counter fraud, local security management and advisory service provider which is hosted by York Teaching Hospital NHS Foundation Trust and supported by a consortium of NHS statutory bodies.

If you would like to read more about Audit Yorkshire please visit our website:

https://www.audityorkshire.nhs.uk/

If you would be interested in knowing more about the services that we could provide to your organisation please contact Audit Yorkshire using the following email address:

yhs-tr.audityorkshire@nhs.net

Fraud Prevention 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 can reprint prescriptions?	
Are all staff advised to lock their computers when they leave their desks?	
Do you audit reprints of prescriptions to identify trends *(e.g. same patient reporting missing prescriptions, same employee reprinting scripts for specific medications)?*	
Do you have a process to flag patients who repeatedly report lost or misplaced prescriptions?	
Are patients who are flagged up signposted for support or offered alternatives such as electronic prescriptions?	
Are relevant staff aware of how to flag a patient's record so that if they contact out of hours services, the call taker will be made aware of any issues / concerns?	
Are all members of staff aware of how to raise a safeguarding concern if it is suspected that someone else is intercepting the patient's prescriptions?	
Unused prescription forms are securely destroyed and serial numbers recorded.	
Only essential prescription forms are taken on home visits, and are kept secure at all times.	

Patient ID Checklist	
Are patients asked for proof of identity / address when registering?	
Are patients who fail to supply proof of ID / address followed up when booking appointments?	
Are staff aware of how to signpost patients with no proof of ID / address to relevant support agencies?	

Practice Funds Checklist	
Are financial responsibilities clearly defined and shared amongst appropriate staff?	
Are segregation of duties in place *(e.g. different staff raise orders / approve payments)?*	
If unable to use segregation of duties, are any transaction level limits in place?	
Are all payments to suppliers reconciled against invoices before being made?	
Are documentation procedures in place? *(e.g. remittance advice slips / deposit slips are used, filed and available for audit)*	
Have you reviewed your bank mandate to make sure only current staff are named?	
Is there a reconciliation process in place to regularly compare bank statements to other internal records?	
Do partners review cheque payments?	
Are staff duties rotated, and all staff encouraged to take their annual leave?	
Are any spot checks conducted on practice accounts and financial records?	
Are comprehensive procedure notes available for relevant staff, outlining processes for dealing with income, expenditure, payroll etc?	
Do you review payroll records to ensure salary payments are genuine? C*onsider exception reporting which will alert you to payments < 10% higher than the previous month.*	
Have partners got access to the Payroll system in order to complete spot checks?	
Do you have an Anti-Fraud, Bribery and Corruption Policy and do staff know how to report concerns?	
Do you obtain independent assurance that pension contributions have been received by the NHS Business Services Authority?	
Is the person responsible for practice submissions to NHS Pensions making submissions for their own pension? If so, seek additional sign off from an independent person and ensure a note to that effect is stored.	

Mandate Fraud, Office Supply Scams, and Phishing Checklist	
Do staff members who make payments to suppliers know about Mandate Fraud and how to spot phishing emails? *(If not, consider signing up to a Fraud Prevention Masterclass - contact the ICB's LCFS for more information)*	
Is there a set procedure in place to follow if a request is received for supplier's bank details to be updated, or if an unusual payment request is received from a colleague?	
If a request for bank details to be updated or an unusual request is received, do staff know to make contact with the supplier using an established phone number, to verify the request?	
Are emails requesting invoice payments / changes to bank details closely scrutinised?	
Do your staff know how to report concerns if they are worried about an unusual request?	

Pre Employment Checks Checklist	
Do recruiting staff refer to the NHS Employers website for guidance?	
Are new starters required to bring their original identity documents / qualification certificates on their first day?	
Has the practice considered what to do if a new starter fails to bring their documents?	
Are qualification checks completed whenever proportionate to do so?	
Do you ensure agency workers provide proof of ID on arrival?	

Further Fraud Awareness Training

The Audit Yorkshire Counter Fraud team run a series of Fraud Prevention Masterclasses over Microsoft Teams. Topics covered include Cyber Enabled Fraud, Fraud Awareness for Finance Staff, Recruitment Fraud, Payroll Fraud, Procurement Fraud, Fraud in the NHS, Fraud Awareness for Managers and Fraud Awareness for HR.

You can also sign up to receive our monthly Counter Fraud Newsletter direct to your inbox.

For more information, please contact the ICB's Local Counter Fraud Specialists (our contact details are on page 9).