# COUNTER FRAUD GUIDANCE FOR GP SURGERIES

## Introduction

Understandably, fraud isn't the first thing you think about when you consider a career in the health service. Most people who join the NHS are surprised to learn that their organisation has a dedicated Local Counter Fraud Specialist.

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 money lost to fraud in the NHS in a single year 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.

If you have any questions on the contents of this guide, please don't hesitate to contact the CCG's Local Counter Fraud Specialists, Rosie Dickinson (rosie.dickinson1@nhs.net / 07825 228 175) or Steve Moss (steven.moss@nhs.net /07717 356707)

## What is fraud?

Fraud is a criminal offence which is generally quite well understood but does often get confused with theft. 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. Another example would be if a job applicant filled in an application form claiming that they held a particular qualification which they don't possess.

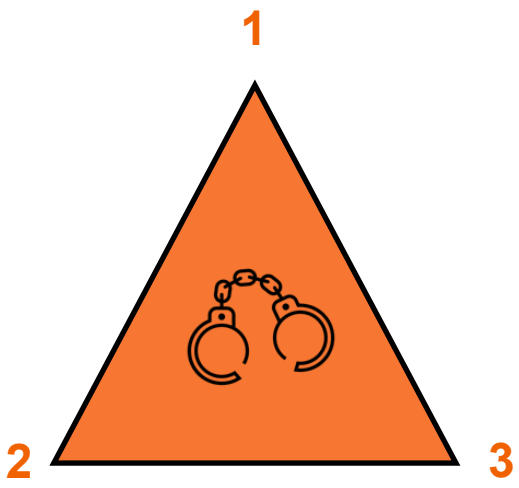
**Fraud by failure to disclose** - this offence applies where somebody fails to disclose information which they are legally expected to share. A good example of this is the section of a job application form where the applicant is asked to share any existing convictions or pending charges.

**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. That could be access to a bank account, authority for making decisions about which contractors are awarded NHS contracts, or access to computer systems containing patient data. 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?

In the 1950s a criminologist called Donald Cressey developed his own theory of how fraud takes place. He suggested that three factors needed to be present in order for fraud to take place.




### The Fraud Triangle

1. **Opportunity** - there needs to be a window of opportunity, or a system weakness for fraud to occur
2. **Pressure** - the individual committing the offence needs to be under some form of pressure (e.g. in debt, struggling to make ends meet, dealing with stress or addiction)
3. **Rationalisation** - the individual needs to find a way of justifying their actions

You might be wondering what a 1950s criminology model has to do with your practice. It's useful to be aware of this theory as it provides the key to protecting your surgery.

Arguably, you have the most control over the **Opportunity** section of the fraud triangle. By reading through this guidance, you should be able to check your surgery for areas of opportunity which could be exploited. By following the **checklists** at the end of this document, you should be able to produce an action plan for reducing opportunities for fraud to impact your surgery.

It is also important to recognise the role of **Pressure** in the fraud triangle. For example, if a patient is repeatedly claiming to have lost their prescription, there may be a safeguarding issue which is underlying this. They may be struggling with an addiction or could be facing exploitation from a relative 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** may target NHS accounts teams, and unfortunately, a very small minority of **NHS staff** will attempt to defraud their employer.

## 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.

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

### Prescription Fraud Case Studies

#### Lisa Rowles

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

#### Ashleen Murray

Stole a prescription pad during an appointment with her GP

Filled out and forged signatures on 22 prescriptions

Redeemed the prescriptions at pharmacies across a large area

Found guilty of 3 counts of Fraud by False Representation

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 in which patients who have been sent to prison have arranged for **associates** to attend their GP practices in order 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. Practice funds 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 is 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.

### Practice Funds Case Study

#### Karen Evans

Karen was employed as a practice manager by a GP surgery in Manchester.

Within a month of starting her role, she had started to siphon off practice funds.

She falsified hundreds of patients records over a 15 month period. This even included marking several patient records as "End of Life Care", despite these patients not being on the End of Life pathway.

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. This began an internal investigation which eventually 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 also defrauded a previous GP practice of £77,000 by claiming that the money had been used to pay for medical supplies.

As a result of Karen's actions, 4 of the 5 GPs at the practice had to step down or take early retirement. The patients whose files had been marked as End of Life had been badly affected too as they were caused significant distress by her actions.

Karen was sentenced to 3 years and 4 months in prison.

# Current Fraud Trends Affecting the Whole NHS

## Mandate Fraud

Mandate Fraud occurs when a fraudster **impersonates a genuine supplier** and requests that the bank details held on file are updated. This results in future invoices being paid into the **wrong bank account.**

Mandate Fraud is very appealing for fraudsters. It can be executed remotely and has a very real potential to result in **a massive pay day** for the criminals. Those committing this type of fraud are very determined and will go to significant lengths to fabricate the perfect disguise.

To do this, Mandate Fraudsters engage in **social engineering**. This is the process by which they research their target and ensure that their emails are cleverly designed to try and bypass even the most experienced NHS employees.

The scammer will **lift corporate branding** (including logos, fonts, signature structures etc.) from genuine emails and use this to make their own emails look correct. They may impersonate an **NHS employee**, making contact with the supplier to secure a list of invoices which are due for payment. They can then attach this list when they target NHS staff to lend their email a further appearance of authenticity. They may also try and **compromise an email account** in order to find out which names they need to drop into their communications with you, and can fabricate multiple fake email accounts from which they can pose as several genuine supplier employees.

During the Covid-19 pandemic, we have seen numerous attempts to target NHS organisations in the Yorkshire area. Some of these attempts have been extremely close to home, and very well constructed. We have had reports of these frauds being attempted against Trusts and CCGs in the local area. Unfortunately, **there is no reason** why a Mandate Fraudster would not target a GP surgery.

Please see the checklists at the end of the document to learn more about how to prevent Mandate Fraud from affecting your practice.

### Mandate Fraud Case Study

#### Mersey Care NHS Foundation Trust

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

Criminals entered into communication with 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.

## Phishing

Mandate fraud is just one example of how phishing emails can target NHS organisations. 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 and how to access specific training on this

### 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 a few days earlier. It featured their official logo and claimed she had an overdue bill which was due to become very steep as late fees were about 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 a spoofing software to disguise their real number by making it look as though they were calling from Halifax customer services.

Fortunately, she has now been refunded the money.

## Social Engineering Risks at GP Surgeries

Social Engineering is a cyber security term which refers to the use of psychological tactics which are used to influence the behaviour of others. When we're talking about NHS Fraud, we tend to mean the methods that a fraudster uses to manipulate NHS Staff into taking risky actions, such as making payments outside of normal policies, processes and procedures.

Social Engineering is often tied up with phishing, the distribution of malicious software, fake invoice payments, and mandate fraud. In cases of mandate fraud, social engineering tactics tend to include lifting corporate branding, invoice templates, and personnel names from a genuine supplier. These details are then used to target NHS organisations, making it appear as though the supplier is making a genuine request for their bank account details to be changed.

In invoice payment fraud, the fraudster may impersonate NHS staff as well as suppliers. Their goal is to encourage employees to make payments, download files, or provide access credentials by appearing to be a known and trusted colleague. This can be through several methods:

1. Creating a fake email address which is a close match to an NHS employee
2. Using software to "spoof" an email address (so that when emails arrive, on the surface it looks like they have come from a recognised sender)
3. Compromising an NHS employees genuine work email account, usually via a phishing email

In order to be successful, the fraudster needs to know who to impersonate. When looking at NHS Trusts, fraudsters often impersonate high profile staff, such as CEOs or Finance Directors. These people are easy to identify as they are publically visible. Impersonating senior staff places extra pressure on the email recipient. They may feel compelled to comply with an unusual request if it appears to have come from someone who is senior to them.

Most GP surgeries have a patient facing website which lists the name of the Practice Manager and GP Partners. It is likely that invoice payment fraudsters will impersonate these individuals on the basis that they are most likely to be able to request and authorise payments. Fraudsters may target an entire practice using a phishing email, as one compromised account can be a rich source of information.

Once an account has been compromised, it can be used to find out the names and contact details for colleagues, to identify key contacts at suppliers, and to gain an understanding of how payment requests are usually processed.

### Social Engineering Case Study

#### Fake Invoice Authorisation

A member of staff at a GP practice received an email from the Practice Manager. The email was a request for the urgent payment of an invoice to a new supplier. In the email trail which was forwarded, a GP partner had authorised the payment.

The invoice, worth tens of thousands of pounds, was paid. However, the Practice Manager and the GP Partner's email accounts had been compromised, and the new supplier did not exist.

# Cyber Security Advice

## Phishing Emails

Phishing emails are likely to imply that you should or must click on a link contained within the email. When you click on these links, you will be sent to a phishing website where your log-in credentials and / or personal details are harvested. Please avoid clicking on links in emails.

Phishing emails are often used to steal user names and passwords. The most appealing account for a fraudster to gain access to is your email account. This is because your emails contain a lot of sensitive and valuable information. In addition, if you forget your log in details for your other accounts or systems, the reset procedure is likely to include sending you an email to allow you to reset your password.

## Passwords

- It is really important that you follow best practice advice on passwords. If a cyber criminal gains entry to one of your accounts that can lead to other accounts being compromised.
- Do not recycle passwords, each account should have a separate, strong 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
- When updating your password, avoid just changing one detail (e.g. examplepassword1, examplepassword2, examplepassword3)
- We do not recommend that you replace letters in words with numbers (e.g. Pa55word) as this tactic is well known to cyber criminals and does not increase your password security
- 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.

## Multi Factor Authentication

If Multi-Factor Authentication (MFA) is available, we recommend that you turn it on. MFA is an additional security feature which requires you to provide two pieces of information to prove your identity when logging into your account.

If you use online banking, you may be familiar with MFA already. Many banks ask you to log in using a username or customer ID, then to use a bank issued card reader to generate a one-time passcode.

Other MFA options include using a fingerprint scanner, PIN code sent via text or email, or the use of specific authentication apps to approve log in attempts. This means that even if your password is stolen, your account cannot be accessed without providing another form of evidence.

## Pre Employment Checks

The pre-employment check process is absolutely vital to protecting the **security** of your practice and the **safety** of your patients. The process can sometimes seem like a paper exercise, and it may be tempting to push through and get the new starter on board. However, it is always worth reminding any staff who deal with recruitment the real reason why these checks are so important.

The checks are designed to verify the **identity** of the applicant, to ensure their **qualifications** are genuine and valid, and to establish whether the person has any **criminal convictions/pending charges** which would affect your decision to appoint them.

During the Covid-19 pandemic, the process of checking identity documents/qualifications and conducting interviews has been altered. In response, NHS Employers have released updated **guidance** which your staff should be aware of.

It may surprise you to learn that you can buy fake qualifications off eBay (where they are listed as a "novelty item"). There are also some hairraising stories out there about people who failed to disclose their criminal history when applying for NHS roles (for example, Craig Alexander, who was employed by NHS Brent after he failed to disclose that he had recently served a prison sentence for armed robbery).

### Pre Employment Checks Case Study

#### Zholia Alemi

Zholia Alemi was employed in the NHS as a Consultant Psychiatrist for around 22 years. Originally from New Zealand, she had arrived in the UK in the mid 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.

Zholia 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.

Zholia was sentenced to 5 years in prison for her attempt to alter the will of her patient. In addition, she has recently been 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 fabricated qualification certificate.

Zholia did not hold the right qualifications for the role she was carrying out for the NHS. There has already been one inquest into the death of a patient who had been in her care.

## 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.

### 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.

### NHS Employers

Click the link above to locate the latest guidance on pre-employment checks. You'll find detailed advice on various relevant topics such as how DBS checks are being carried out during the Covid-19 pandemic.

### 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.

### 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.

### Action Fraud

A national organisation providing advice on all aspects of fraud. This is a useful resource for any patients, as there have been numerous scams throughout the pandemic in which NHS services (including GP surgeries) have been impersonated to defraud vulnerable people.

## Further Advice and Guidance

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

Rosie Dickinson, Local Counter Fraud Specialist rosie.dickinson1@nhs.net Tel: 07825 228 175

Steve Moss, Local Counter Fraud Specialist steven.moss@nhs.net Tel: 07717 356707

If you have a suspicion of fraud are unsure of where to report it please feel free to contact Rosie and Steve for advice.

## Who Investigates Fraud at GP Practices?

It can be a little bit complicated establishing who will investigate an allegation of fraud where a GP surgery has been targeted. The interaction between GP Practices and a Local Counter Fraud Specialist usually arises when:

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

- The CCG has concerns about the possible misuse or abuse of **CCG 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 or Steve for advice and signposting. Please see the previous page for our contact details.

## About Audit Yorkshire

The CCG'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:

audityorkshire@york.nhs.uk

# 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? | |

| Patient Identity Fraud Checklist | |
|---|---|
| Are patients asked to provide proof of identity and address on registering? | |
| Are patients who fail to supply proof of ID/address followed up when booking appoint-ments? | |
| Are surgery staff aware of how to signpost patients with no proof if ID/address to relevant support agencies? | |

| Practice Funds Checklist | |
|---|---|
| Are financial responsibilities clearly defined and shared amongst appropriate staff? | |
| Are segregations of duties in place (e.g. different staff raise purchase orders and approve invoice payments)? | |
| If unable to use segregation of duties, are any transaction level limits in place? | |
| Are all payments to suppliers reconciled against invoices received 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 ensure 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 all salary payments are genuine? If possible, consider exception reporting which will alert you to payments that are over 10% higher than in 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? | |

| Mandate Fraud, Social Engineering and Phishing Checklist | |
|---|---|
| Do staff members who make payments know about Mandate Fraud and how to spot Phishing emails? *(consider signing up to a Fraud Prevention Masterclass if not)* | |
| 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 payment request is received, do staff make contact with the requesting person by telephone to verify the request is genuine? | |
| Are emails requesting invoice payments or changes to bank details closely scrutinised? | |
| Do your staff know how to report concerns if they are worried about a request for changes to bank details or if unusual requests for payments are received? | |

**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
- Use of pressure - 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. if you click on a link

| Pre-Employment Checks Checklist | |
|---|---|
| Are recruiting staff aware of the updated guidance from NHS Employers? | |
| Are your new starters required to bring their original identity documents and qualification certificates on their first day? | |
| Has the practice considered what do if a new starter fails to bring their documents? | |
| Are qualification checks completed wherever proportionate to do so? | |
| Do you ensure that agency workers also provide proof of identification on arrival? | |