SEPTEMBER 2024

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

NHS FRAUD RISKS SPECIAL

Welcome to a special edition of the Counter Fraud Newsletter. This month we're looking closely at some of the top fraud risks faced by the NHS.

This issue aims to highlight the key risks that threaten our organisation and the integrity of our services. Whether it's identity fraud, payroll fraud, or cyber fraud, these risks can undermine patient care, waste valuable resources, and damage public trust.

By identifying and understanding these risks, we can better protect our services and ensure that every penny is spent on what matters most – patient care.

Throughout this edition, we'll delve into some of the most prevalent types of fraud within the NHS and provide insights into how staff at all levels can help detect and prevent fraud before it causes harm.

Together, we can safeguard the NHS from those seeking to exploit it and ensure that resources continue to be used where they're needed the most. Thank you for your continued commitment to the fight against NHS fraud.

Ways you can get involved

Flag up Fraud Risks

If you think you've spotted a fraud risk in your department please let us know. We will look at putting measures in place to reduce the risk and protect NHS funds.

You can find our contact details in your organisation's Anti Fraud, Bribery and Corruption Policy.

Policy Reviews

If you're creating or updating a policy or procedure, and it'd be helpful to get a counter fraud perspective get in touch with your Local Counter Fraud Specialist.

We're always happy to help make sure that policies and procedures are as fraud proof as possible.

Learn more about NHS Fraud

Reading this newsletter is a great place to start.

You might also find our fraud prevention masterclasses helpful. Please get in touch with your Local Counter Fraud Specialist for more details.

Imposter Workers

Imposter workers are people who arrive on site to work, but are not the person we were expecting. The risk of this happening is higher with agency or bank staff.

In November 2023, we saw headlines of "Bogus nurse stole medical details from Fife hospital" which detailed how somebody posed as an agency worker then stole patient data - read the article here.

We also saw how somebody posed as a nurse to access a children's ward - read the article here.

Over the last few years, the Counter Fraud Team has been made aware of instances whereby a person has registered with an agency, but has essentially then 'sold' shifts and a different person has turned up to do the work.

We have found that this has usually been because the person who actually does the shift has no right to work in the UK and therefore could not have registered themselves, and/or the person selling the shifts takes a proportion of the payment for the work.

To a lesser extent, but equally as concerning, the same tactic has been used by new substantive employees when someone is interviewed, provides correct documents but then a different person turns up to undertake the role.

If a person who isn't appropriately qualified or vetted works on site without our knowledge, although there is a risk to NHS finances, the greater concern is the potential harm that could be caused to patients in our care and the safety of our staff. There is also a risk that the person attending to work may not be a willing participant, and could be a victim of modern slavery.

It is recognised that NHS organisations will always have a need for agency staff, or bank workers, to cover staffing shortfalls. Whether because of an unfilled vacancy, or to cover substantive staff absence.

Please see the blue box which covers advice from NHS Employers and useful resources to lower the risk of this fraud methodology.

Fraud Risk Prevention

NHS Employers advise that all staff, whether substantive or bank / agency, provide some form of personal ID on their first day.

Work based ID cards, i.e. from an agency are not acceptable as a sole form of ID as they do not contain watermarks, holograms or other security markings and can easily be amended / replicated.

Whilst employing agencies work to strict standards to ensure that anybody on their books has undertaken a rigorous recruitment process, they cannot guarantee that the same person will turn up to do the work.

For this reason, the overarching responsibility for ensuring safe working falls to the employing organisation, who must check credentials of every worker supplied to them.

Further information can be found on the NHS Employers website and on the links below.

NHS Employers - Working With Agencies Top Tips

NHS Employers - Background Information on Employment Checks Standards

NHS Employers - Identity Check May 2022

NHS Employers - Employment Check FAQs

Recruitment Fraud

Recruitment fraud covers a whole host of misdemeanours, from misrepresenting skills and experience, failing to disclose a criminal conviction to providing fake ID. Please don't skip this article if you think it's just for Recruitment Teams, there's helpful information for everyone.

The amount of information and documents which are obtained during the recruitment process provides many opportunities for the applicant to lie.

There is not only the risk of fraud, but safeguarding concerns too if somebody gets a job who are not who they say they are, or they don't have the right skills and experience.

Take the case of the doctor who lied about his age and would have started his medicine degree at the age of 10 if his CV were to be believed **(warning, this article may be upsetting to some people)** - Oldham doctor jailed for killing patient in botched procedure - BBC News

Also see our article on Imposter Workers for more details.

Job seekers are also targeted by organised criminals, and there has been a rise in fake job adverts recently.

Fraudsters may post job adverts on social media, or may contact you directly with an amazing offer. The people posting the fake advert will either ask you for personal details which can be used for other frauds, or they ask for upfront payments for "training", "uniform" or "background checks" to trick you into losing money.

To avoid being a victim of this kind of fraud:

- Be wary if you are sent details of a job you have not asked for.
- Research the company you are applying to and contact them directly from details available online, rather than using contact details on the advert.
- Unrealistic salaries or benefits packages can indicate that the offer is not genuine.
- Use reputable recruitment platforms if you are looking for employment elsewhere.
- Minimise what information about you is available to the public.
- Be extra careful if you are asked to part with money upfront.

Fraud Risk Prevention

For anybody in a recruitment team, or if you are a line manager involved in either the onboarding process, or you check the ID of new starters, we would welcome you to one of our Recruitment Fraud Masterclasses.

These hour long sessions will help you gain confidence in checking official documents and ID as well as looking at CV issues, problem references and spotting fake qualifications.

To sign up for a session, please get in touch with your Local Counter Fraud Specialist. You'll find our contact details in your organisation's Anti Fraud, Bribery and Corruption Policy, and / or on your staff intranet.

If your entire team would like to access the masterclass to refresh their knowledge and awareness, please do let us know and we can look at arranging a bespoke session on a date / time to suit you.

Mandate Fraud

Mandate fraud is a type of scam that targets organisations like the NHS by tricking staff into changing bank account details for suppliers, contractors, or employees.

This kind of fraud typically happens when a fraudster pretends to be from a legitimate supplier or service provider. They contact a staff member, often by email, and request that future payments be sent to a new bank account – one that the fraudster controls.

Once the change is made, any payments meant for the genuine supplier are diverted into the fraudster's account. This could involve large sums of money, and by the time the fraud is discovered, the funds are usually gone.

When mandate fraud is successful, the consequences can be severe. The NHS could lose substantial amounts of money, which directly impacts our ability to provide patient care and maintain vital services.

Some of the fraudsters who send mandate fraud emails do an awful lot of research before making an attempt.

They may use social media such as LinkedIn to identify key NHS staff. They can find information on our suppliers via NHS and supplier websites or using press coverage.

They may hijack email accounts used by our staff or suppliers, in order to get hold of invoices, bypass security filters, and to lift logos, branding and email signatures. If they can't hijack an email account, they will "spoof it" - making an email address which nearly matches the genuine one.

Some tell tale signs of a mandate fraud include:

- **Urgency or pressure** - the email might suggest that a change needs making as soon as possible.
- **Email addresses** - you might notice that an email address has changed slightly. Please be aware that even if the email has come from the correct account, the fraudster could be using a hijacked email address.
- **Missing contact information** - fraudsters who hijack genuine accounts or who have copied email signatures usually remove or replace the real suppliers phone number with their own.
- **Timing** - mandate fraudsters are often most active when the NHS is at its busiest, such as the summer holidays, the festive period from November to January, and at the financial year end.

Fraud Risk Prevention

Verification - if you receive an email asking you to change a supplier's bank details, this must be verified before any changes are made.

The safest way to do this, is to contact the supplier using an established phone number. If you don't have one on file, find the supplier's customer services number and ask to be transferred to the relevant team.

Don't engage - don't use contact details from within the email to verify the request. The account could be under the control of a fraudster, and they may have replaced genuine phone numbers with their own.

Policy and Procedure - it is vital that you follow your organisation's policies and procedures. These are in place to protect NHS funds from fraud.

Report it - if you receive a suspicious email asking for bank details to be changed, please report it to the Local Counter Fraud Specialists (LCFSs). You'll find contact details for your LCFS on the last page of this newsletter.

Refresh your awareness - if you work in finance or if you have the ability to make payments at work, then please consider coming along to our Creditor Payments and Cyber Enabled Fraud Masterclasses. You can find out more by contacting your Local Counter Fraud Specialist. Check your organisation's Anti Fraud, Bribery and Corruption Policy for contact details.

Working Whilst Sick

The Counter Fraud Team receive referrals about loads of different kinds of NHS Fraud, but by far our most common referral is what we call "Working Whilst Sick" (often shortened to WWS). This is also the most common referral type nationally, making up almost a quarter of all NHS counter fraud referrals in 2023 / 24.

This type of fraud occurs where a person falsely claims that they are too unwell to attend work. Whilst signed off and receiving NHS sick pay, they go and work somewhere else. This results in them being paid twice for the same period of time.

The person might pick up bank shifts at a neighbouring organisation, do similar work at a non-NHS employer, carry out self-employed work, or do something completely different. Whether or not it is viewed as fraud depends on the specific circumstances.

Reports on this type of fraud cases tend to pop up in the press - for example, this case where a doctor was struck off for working as a locum whilst signed off sick,

Fraud Risk Prevention

For all staff

- You must tell your line manager about any secondary employment. This is not just for WWS purposes, but for other reasons too, such as making sure that working time directives aren't breached.
- Your contract of employment may require that you seek permission from management before agreeing to any outside employment. Make sure you know what is expected of you.
- Your organisation's Conflicts of Interest Policy, Standards of Business Conduct Policy, and / or Sickness Policy is likely to state that you must formally declare any secondary employment. Your organisation might have different names for their policies, so if you want to check your local policies and don't know where to start, contact your LCFS or HR team.
- If you are intending to work elsewhere whilst signed off sick, tell your line manager and / or occupational health (your HR team will be able to advise)
- Tell your GP if they you have a second job and they are going to issue you with a fit note. Ask them to make it clear on your fit note whether you are unsuitable for any work, or if your illness only affects one of your roles.
- Find out more about fraud in the NHS by attending one of our General Fraud Awareness Masterclasses.

For Line Mangers

- Ask your teams about outside work at least annually and keep a record of any secondary employment they have.
- If you suspect that a member of staff is working whilst sick, please contact your LCFS for advice before you do any fact finding yourself.
- To learn more about working whilst sick, and other types of fraud which you may come across, sign up for one of our Counter Fraud for Line Managers masterclasses.

REPORTING FRAUD CONCERNS

Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please **notify your Local Counter Fraud Specialist**. You'll find our contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy,.

You can also report your concerns to the **NHS Counter Fraud Authority** using their online reporting tool or phone number: 0800 028 40 60.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

Suspicious Emails

Do not click on any links or attachments.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the LCFS team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Action Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details can be found in your organisation's Anti-Fraud, Bribery and Corruption Policy.