AUDIT YORKSHIRE

September 2026

Counter Fraud Newsletter

Welcome to this month's edition of the Counter Fraud Newsletter for NHS staff. You will find contact details for your Local Counter Fraud Specialist in your organisation's Anti-Fraud, Bribery and Corrruption Policy.

Overseas Patients: Helping Protect NHS Funds

The NHS is a residency-based health system. Where a patient is an overseas visitor and no exemption applies, NHS organisations must identify this and recover the appropriate charges.

Who is an overseas visitor?

An overseas visitor is someone who is not "ordinarily resident" in the UK. Broadly, this means they are not living here lawfully, voluntarily and for settled purposes as part of their regular life.

Someone may be an overseas visitor if their main home is outside the UK and they are here temporarily. British citizens who normally live abroad can also be overseas visitors. Paying UK taxes, registering with a GP or having an NHS number does not, by itself, confirm entitlement to free NHS hospital treatment.

Urgent or immediately necessary non-elective care must not be withheld or delayed while eligibility or payment is investigated. Patients who are not ordinarily resident may need to pay in advance for elective treatment unless an exemption applies. Access to primary care is unaffected.

What should you look out for?

Please raise concerns early if, for example, a patient:

- Provides an overseas address or asks for correspondence to be sent abroad;
- Uses an overseas telephone number for follow-up appointments;
- Says they are visiting the UK or have only recently arrived;
- Cannot provide evidence that they live in the UK on a settled basis; or
- Provides travel insurance documents or asks about reclaiming treatment costs.

Unsure?

If you think a patient may be chargeable, contact your organisation's Overseas Team.

They will review eligibility and any exemptions sensitively and in line with national guidance. Concerns can be raised anonymously.

If you suspect that someone is deliberately providing false information, contact the Counter Fraud Team or mention this when referring the matter to the Overseas Team.

Recruitment Fraud: Why Checks Matter

A former NHS employee has been jailed for four years after fraudulently obtaining NHS roles by making false claims about his qualifications, employment history, professional memberships and references.

The NHS Counter Fraud Authority (NHSCFA) reported that he falsely claimed to have graduated from the University of Oxford and secured a number of NHS positions using dishonest information.

Once in post, he would go off sick and remain absent until his contract was terminated, meaning he did little work and did not gain the experience he claimed to have in future applications.

The investigation found that he had fraudulently obtained 13 NHS employments, resulting in a confirmed financial loss of **almost £170,000** to the NHS.

How was the fraud discovered?

Routine pre-employment checks identified discrepancies in the applicant's claimed employment history. Further enquiries revealed that:

- A claimed NHS role had never been held.
- References provided were not genuine.
- Claimed qualifications could not be verified.
- Claimed professional memberships did not exist.

You can read more about this case on the BBC news website: NHS fraudster who lied about going to Oxford University jailed - BBC News

Key Reminders for Recruitment Staff

✅ **Verify qualifications and professional memberships**
Where qualifications, registrations or memberships are essential for a role, ensure they are independently verified.

✅ **Scrutinise references carefully**
Do not assume references are genuine. Follow local procedures and verify concerns through appropriate channels.

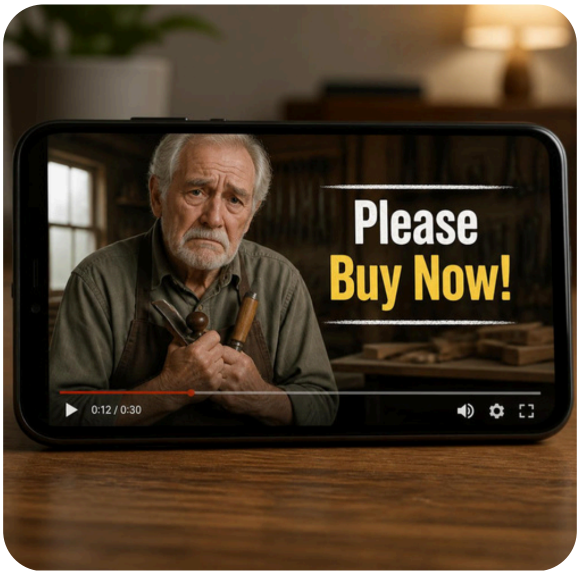
✅ **Check employment history thoroughly**
Follow up unexplained gaps, inconsistencies or information that cannot be independently verified.

✅ **Complete all identity checks**
Identity verification remains a key defence against recruitment fraud and should be completed in line with NHS guidance and local procedures.

✅ **Trust your instincts and escalate concerns**
If something doesn't seem right, seek advice and escalate concerns through the appropriate route rather than proceeding on assumptions.

If you identify or suspect recruitment fraud, please report your concerns to your Local Counter Fraud Specialist. Please see your organisation's Anti-Fraud, Bribery and Corruption Policy for details.

Beware AI-Powered "Sympathy-Baiting" Shopping Scams



Social media is increasingly being used by fraudsters to promote fake products through AI-generated videos designed to tug at people's heartstrings.

These scams, often referred to as "sympathy-baiting" scams, typically feature an apparently elderly person, struggling craft worker, young entrepreneur, or someone facing hardship who claims that nobody is buying their handmade products or that they desperately need support.

The videos can be highly convincing and often show a person seemingly making beautiful handcrafted items, accompanied by emotional stories about financial difficulties, bullying, illness, or other hardships.

In many cases, however, the videos, voices, and stories have been generated or manipulated using artificial intelligence. The goods themselves are mass produced and often low quality, rather than bespoke hand crafted items as described or shown in the video.

Consumer organisation Which? has warned that suspicious accounts promoting these products have appeared across major social media platforms, including Facebook, Instagram, TikTok, and YouTube. You can read more on the Which? website.

Spot the Warning Signs

Audio that sounds robotic, unnatural, or out of sync with the speaker's mouth movements.

Overly emotional or repetitive stories designed to provoke sympathy and urgency.

Claims that "nobody will buy my products" or that the seller is being unfairly treated.

Multiple accounts sharing identical videos, products, or stories.

Limited contact details or vague information about who is operating the business.

A website claiming to be a small local business, but with shipping or return addresses located overseas.

Protect Yourself

Before making a purchase, consider the following steps:

Research the seller independently rather than relying solely on social media adverts.

Read reviews from multiple sources and look for genuine customer feedback.

Check the business's contact details, returns policy, and physical address.

Be wary of deals that seem unusually cheap or videos that rely heavily on emotional appeals.

Use a credit card or another payment method that offers consumer protection where possible.

If something does not feel right, trust your instincts. Taking a few moments to verify a seller could prevent you from losing money to an AI-powered scam.

Fraud Awareness & Prevention Training

Our Fraud Awareness and Prevention Training is practical, engaging, and open to all NHS staff – no prior knowledge needed.

Designed around real NHS risks, these sessions give you the confidence to spot fraud, understand the warning signs, and know exactly what to do if something doesn't feel right.

We cover a wide range of key topics, including fraud fundamentals, procurement risks, cyber-enabled scams, payroll and expenses fraud, and tailored sessions for finance, HR, and managers. You can also learn about recruitment fraud, ID checking, and wider fraud risks across the NHS.

Fraud affects us all—and every member of staff has a role to play. Join a session to build your confidence, protect NHS resources, and help safeguard patient care.

Recruitment and ID Checking	3rd December 3pm
Cyber-Enabled Fraud	17th November 10am
Introduction to Fraud Prevention	5th January 10am
Fraud for Finance Staff	9th December 2pm
Fraud Awareness for HR	On request - please contact us
NEW Imposter Workers and ID checking	On request - please contact us
Procurement Fraud	20th October 10am
General Fraud Awareness	9th October 11am
Payroll Fraud	22nd September 1pm
Fraud Awareness for Managers	4th November 11am

The sessions are delivered over Microsoft Teams and last around 1 hour. If you would like to book a place on any of the training, please contact: **yhs-tr.audityorkshire@nhs.net**

Bespoke Training Sessions
The Local Counter Fraud Team are always happy to pop along to speak to individual teams.

If you would like us to attend one of your team meetings, to deliver a training session on a key fraud risk area, or for any other fraud prevention advice, please contact us using our details (which you'll find on the last page).

REPORTING FRAUD CONCERNS

Fraud against 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 Counter Fraud 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 **Report 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.