AUDIT YORKSHIRE

October 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 Corruption Policy

The Illusion of Credibility

Fraud is not always about stolen money, it can begin when someone uses false information to gain access or opportunities they have not earned.

Across the UK, individuals are using false identities, qualifications, employment histories and references to secure jobs or access systems and information.

Why Does This Matter?

Healthcare staff may have access to patient information, secure areas, equipment and public funds. Dishonesty during recruitment can therefore put patient safety, public confidence and NHS resources at risk.

What Should Staff Look Out For?

- References that cannot be independently verified.
- Inconsistencies in employment histories or qualifications.
- Attempts to bypass established procedures.
- Unusual requests for access. For example - equipment, computer records and systems, or access to unauthorised areas.

One warning sign does not prove wrongdoing, but it may justify further checks.

Everyone Has a Role to Play

- Everyone has a role in protecting NHS resources.
- Asking a question or raising a concern is not an accusation; it allows the appropriate checks to be made.
- Fraudsters often succeed because they appear credible.
- Trust is not a control: robust checks, established procedures and professional curiosity help prevent false information from going unchallenged.

SPEAK UP!

If something doesn't look right, speak up. A quick conversation today could prevent a much bigger problem tomorrow.



Don’t get caught out by copycat websites

Fraudsters are setting up fake websites hoping to tempt people to access them after doing a Google search for genuine websites. These copycat websites imitate official services and often charge people unnecessary fees to process or renew documents which would usually be free if accessed via the official websites. They may appear near the top of search results as paid adverts, so be aware and avoid assuming the first result is the official site.

Key warning signs include:

- A web address that looks official but does not use the correct official domain, such as gov.uk for UK government services.
- Wording in the small print that says the site is not affiliated with the official organisation.
- Pressure to complete forms or make payments quickly.
- Requests for personal or payment details on websites that do not clearly show secure browsing.
- Services such as tax returns, passport applications, driving licence renewals, theory tests, ULEZ or congestion charge payments, and ESTA applications being offered through unofficial websites.



For further information, see How to spot a copycat website - Which?



Manager's Minute

Trust, but Verify

Managers work hard to create positive and supportive teams built on trust. However, effective management also requires appropriate oversight. Most issues identified through counter fraud work could have been prevented or identified earlier through routine checks, timely review of records, and asking simple questions when something doesn't seem quite right.



Verification is not about mistrust. It is about protecting public resources, ensuring fairness for colleagues, and maintaining confidence in NHS services. Whether reviewing timesheets, expenses, recruitment documentation, or sickness records, taking a few extra moments to check the evidence can prevent significant problems later.



Help Protect Friends and Family from Telephone Switchover Scams

As the UK moves from analogue to digital landline services, criminals are exploiting the change to target vulnerable people with convincing scams.

The telephone network is undergoing a major upgrade, with traditional analogue landlines being replaced by digital services that operate through a broadband internet connection. While the switchover is legitimate, fraudsters are using it as an opportunity to deceive people into handing over personal and financial information.

How the Scam Works

Scammers may contact individuals by phone, claiming that they need bank details or payment information to complete the switchover. Some may even threaten that telephone services will be disconnected unless immediate action is taken.

These calls can sound convincing and are often aimed at vulnerable people or those who may be less familiar with the changes taking place.



Key Messages to Share

If you have vulnerable relatives, neighbours, or friends, please encourage them to remember:

- Telephone providers will not ask for bank details over the phone to complete the digital switchover.
- The switchover itself does not require someone to provide payment card details during an unexpected call.
- Be cautious of callers who create a sense of urgency or threaten service disconnection.
- Never share passwords, PINs, or banking information with an unsolicited caller.
- If in doubt, hang up and contact the telephone provider directly using a trusted number.

Many scams succeed because victims are caught off guard or feel pressured to act quickly. A conversation with a vulnerable friend, family member, or neighbour could help prevent them from becoming a victim.

By raising awareness of this scam, we can help protect those most at risk and ensure they can benefit from the digital switchover safely.

Halloween – “Don’t let fraudsters trick you”

Fraudsters don’t need a broomstick or a disguise to cause a fright. Often, all they need is an email, phone call or message that catches us off guard.

Be wary of unexpected requests for information, changes to bank details, unusual payment requests or messages encouraging you to click a link or act urgently.



👻 Stop and think before you act.
🎃 Check unusual requests through a trusted route.
🕷️ Never be pressured into ignoring normal procedures.

Professional curiosity is one of our best defences against fraud. If something doesn’t feel right, pause, check and challenge.

This Halloween, make sure the tricks are confined to the trick-or-treaters.

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."