tiaa.

Certified B Corporation
Learn more at bcorp.com



Issue 10

Fraud Stop

NHS Fraudsters
Cases in Court

Fraud Spotlight
Multiple Employment Fraud

Artificial Intelligence
Risks in Recruitment

Introduction

The NHS Counter Fraud Authority (CFA) is a special health authority tasked to lead the fight against fraud, bribery and corruption in the NHS.

In a recently published article, their Chief Executive Officer has stated that fraud accounts for around 4.1 million incidents each year, or roughly 41% of all crime against individuals in England and Wales. As the UK's most common crime, fraud, bribery, and corruption put publicly funded healthcare at risk, diverting resources from frontline services and undermining public trust. It is currently estimated that £1.346 billion of NHS funding is vulnerable. Protecting these resources is essential to delivering safe, effective healthcare and value for taxpayers. The nature of fraud is evolving rapidly, driven by digital technology, complex financial arrangements, and fragmented delivery models.

Everyone has a part to play in fighting fraud. Being aware of the risk and remaining vigilant are the most important first steps, followed by knowing how to report fraud.

Former NHS employee found guilty of fraud after stealing and reselling stock back to an NHS Trust

The NHS CFA reported in July 2026 that they had successfully investigated and secured convictions relating to a £279,000 fraud involving stolen hospital stock being resold back to an NHS Trust.

A former employee of the NHS Trust was found guilty of fraud by abuse of position and fraudulent trading on 30 June 2026 following a Crown Court trial.

Two others were also convicted following the trial for their involvement in the fraud. The first was found guilty of fraudulent trading and the second was found guilty of money laundering through the acquisition, retention, use or control of criminal property.

The former NHS employee was employed as a materials management assistant while one of the other defendants was employed by a different Trust as a healthcare assistant. The third defendant was the director of a company that specialised in medical supplies.

Between October 2016 and September 2019, the materials management assistant stole medical supplies from NHS operating theatre stock rooms and passed the supplies onto the company, who then sold the items back to the Trust. This meant that the Trust was effectively buying back its own stock.

The Trust became suspicious of the company and decided to make its own enquiries. Some of the packages delivered by the company were opened by hospital staff prior to their delivery to hospital theatres.

They noticed that identification numbers on some delivered items matched those of items that had been previously ordered and delivered to the Trust, either by the company or another supplier.

In total, the NHS Trust spent almost £233,000 buying back its own stock.

Including supplied items that were sourced from China which were found to be sub-standard and subsequently had to be destroyed, the company had invoiced the Trust for orders totalling £306,000, although the Trust had withheld some payments due to its suspicions about the company.

Checks made by the Trust showed that the materials management assistant made the request to set up the company as a registered supplier to the Trust and also initiated all of the Trust's business with the company.

The investigation found that funds paid by the Trust into the company's business account were redirected to a shell company set up by the healthcare assistant, and to personal accounts in the names of all three defendants.

The subject of the investigation was sentenced to 8 years in prison after being found guilty of all charges. The Company Director was sentenced to 7 years in prison after being found guilty of all charges and the third defendant, a Healthcare Assistant with the NHS, was sentenced to 30 months imprisonment, suspended for 36 months for money laundering involvement.



Two convictions for lying about qualifications and references

The NHS CFA reported in July 2026 that an investigation had uncovered a fraud in which a former NHS employee dishonestly obtained 13 non-clinical roles across NHS organisations, defrauding the NHS of almost £170,000.

The fraudster was sentenced to four years' imprisonment at Crown Court on 24 July 2026. He had previously pleaded guilty to three charges of fraud by false representation on 18 August 2025.

He was caught after applying and being offered the role of Deputy Chief Operating Officer Urgent Care/ Transformation and Operations at an NHS Trust in 2021. He had claimed in his application to be employed as Director of Transformation and Improvement at a different NHS Trust.

However pre -employment checks on the Electronic Staff Record (ESR) system found no evidence of this and the other Trust subsequently confirmed that they had never employed him.

Further enquiries revealed that the fraudster had submitted false references in support of his applications. One of his referees was fictitious, whilst other references were linked to NHS email accounts which he accessed or controlled.

In his application, he claimed to have been awarded MSc degrees by the University of Oxford and Birkbeck, University of London, including providing a certificate for the latter. However, both institutions confirmed that he did not complete his respective courses.

He also stated in his application that he held memberships with several professional bodies, including the Institute of Directors and the Chartered Management Institute. Enquiries found no evidence that he held any professional memberships.

The fraudster was found to have applied for 2,071 NHS posts, gaining 13 fraudulent employments resulting in a confirmed financial loss of £168,072.41.

A recurring pattern emerged across his NHS roles. Shortly after taking up post, he would go sick and remain absent until his contract ended or his employment was terminated. As a result, he frequently undertook little or no work and did not acquire the experience claimed in his applications.

Two of the charges also related to roles he dishonestly obtained outside the NHS.

In a second case, a woman who lied about holding two degrees to secure a job with an NHS Trust was sentenced at Crown Court on 5 August 2026 to 20 months' imprisonment, suspended for 18 months, after defrauding the NHS Trust of more than £72,000.

She had previously pleaded guilty to fraud by false representation at the Magistrates' Court on 6 July 2026.

In an application for a physical healthcare practitioner role with the Trust in August 2022, the fraudster falsely claimed to hold a BA in Children, Young People and Society from the University of York and an MSc in Advanced Clinical Practice from Teesside University. She was appointed on the basis of having these degrees.

During pre-employment checks, she was asked to provide evidence of her qualifications but claimed that she could not access her certificates because of an abusive relationship.

Following a risk assessment, the Trust allowed her to start work while efforts were made to obtain evidence of her qualifications. She later claimed that she had already provided her advanced clinical practice certificate, but the Trust had not received it.

Investigators contacted the relevant universities, and both confirmed that the BA and MSc courses had not been completed.

Her employment ran from 21 November 2022 until 24 May 2024. During this time, the Trust paid her £72,485.77 in gross pay, employer pension contributions and employer National Insurance contributions.

Former NHS employee who worked elsewhere while off sick receives suspended jail sentence

Following an investigation led by a Tiaa Anti-Crime Specialist, a former NHS Support Worker was sentenced on 13 August 2026 to 12 months' imprisonment, suspended for 24 months, 150 hours of unpaid work, and 15 rehabilitation activity days.

The fraudster pleaded guilty to multiple offences of fraud by false representation relating to conduct between November 2017 and May 2023. The investigation established that, whilst employed by an NHS trust, the individual undertook secondary NHS employment elsewhere via bank during periods when they were recorded as absent through sickness and were receiving occupational sick pay. Evidence showed that 271 shifts were worked elsewhere during periods of sickness absence.

The investigation identified losses of £10,921.47 arising from salary payments made during periods of sickness absence. The offending continued over a period of more than five years and involved repeated opportunities to correct the behaviour.

At sentencing, the court determined that the offences involved a significant breach of trust and that the custody threshold had been crossed. The court noted the seriousness of the offending but also took into account the guilty pleas, admissions made during interview, previous good character and expressions of remorse.

The court also awarded £7,000 in compensation for investigation costs incurred.





Fraud Spotlight

Multiple Employment Fraud

Earlier in 2026, the NHS CFA issued the fraud prevention quick guide on Multiple Employment Fraud for the healthcare sector. NHS CFA reporting data highlights that undertaking undisclosed additional employment alongside a substantive role is a prominent issue within the staff fraud reports category.

Multiple employment fraud is a form of staff fraud that may arise where an individual intentionally undertakes undisclosed or unmanaged additional employment alongside their substantive role, resulting in an inability to meet contractual requirements or working time regulations.

Following the pandemic, working practices changed and many in the healthcare sector now work remotely or as hybrid workers, doing a combination of home and office or site based working a few days a week. Whilst these arrangements benefit and provide flexibility for the workforce, they may also be vulnerable to fraud.

Multiple employment fraud is also referred to as dual working and can include:

- Claiming full-time hours across multiple roles that overlap
- Working in multiple roles simultaneously while being paid for the same period of time
- Failure to disclose secondary employment to avoid scrutiny or conflict of interest
- Using false or misleading information to secure additional roles
- Breaching working time regulations

The risks of an employee working multiple employments include employees making errors due to fatigue and stress, compromised patient care, and financial loss and reputational damage to the employer.

How to spot multiple employment fraud

Unavailability during contracted hours Employees who are frequently unreachable or absent during their scheduled working hours may be working elsewhere while still being paid.

Lack of visibility Employees consistently unavailable to attend in person meetings/events, failing to turn on cameras and unresponsive to calls.

Reduced performance Employees who work excessive hours across multiple roles may show signs of reduced or poor performance. This not only raises concerns about fraud but also poses risks to patient safety and staff wellbeing.

Deliberate non-disclosure of secondary employment Employees who avoid questions about other jobs or fail to declare additional roles may be attempting to conceal conflicting work commitments.

How to reduce the risk of multiple employment fraud occurring

- Adhere to the six NHS Employment Check Standards guidance which covers the essential checks that must be carried out when recruiting staff.
- Organisations should have a policy in place clearly communicating their expectations of employees. This should include the definition of core hours, agreed working patterns, expectations for attendance at the workplace and the expectation for staff to declare any other employment. Usually found in an organisation's code of conduct, secondary employment policy or standards of business conduct policy, the policy should also include the consequences of working elsewhere during contracted hours.
- Procedures should be put in place to inform line managers of their duty to effectively monitor remote workers.
- Organisations should empower their managers to feel confident to have conversations about unusual or poor performance with their staff.
- All contracts of employment should include reference to the requirement to declare any additional employment from the point of recruitment, supported by an annual declaration process.
- Raise awareness through the education/training of all line managers/supervisors on multiple employment fraud risks.
- Create a culture of transparency where staff are encouraged to speak openly about other employment and understand the importance of declaring additional roles.
- If using temporary staffing suppliers, regardless of whether they are on, or off, framework, seek reassurance from those suppliers regarding the recruitment checks they are carrying out on the temporary staff they are assigning to you.

Read the full NHS CFA Quick Guide on Multiple Employment Fraud **here**

Seek advice from your Anti-Crime Specialist if you would like to mitigate the risks associated with multiple employment fraud or contact fraud@tiaa.co.uk

Artificial Intelligence Risks in Recruitment

NHS Employers has identified that the use of Artificial Intelligence (AI) tools is an emerging risk in recruitment, enabling candidates to misrepresent their qualifications, experience, or identity through the use of artificial intelligence tools. Examples include AI-generated CVs, fabricated employment histories, manipulated interview responses, and the use of deepfake technology during virtual interviews. These practices can undermine the integrity of recruitment processes, increase the risk of employing unsuitable candidates, and expose organisations to financial, operational, and reputational risks. Employers should strengthen screening and verification processes to ensure recruitment decisions are based on genuine skills, experience, and identity.

Organisations should consider:

Does the Recruitment Policy (or equivalent) include content regarding the "Acceptable Use of AI by candidates"



Be clear in the policy that the organisation recognises that candidates may use AI tools to improve spelling, grammar, formatting, and presentation of application materials. Candidates must ensure that:

- Information provided remains accurate and truthful.
- Examples, experience, and qualifications are genuine.
- Assessment responses represent their own knowledge and abilities unless otherwise permitted.

Undisclosed AI use that materially misrepresents capability or suitability may be treated as recruitment fraud.

The policy should also be clear that AI tools should not be used by candidates during online interviews

Do application forms require candidates to make a declaration on whether AI tools have been used to complete the application? If AI has been used, is there a further declaration that information provided remains accurate and that examples, experience and qualifications are genuine?

It is fair to say that a large percentage of candidates will use AI – and it can be acceptable as detailed above. Transparency is key and employers should not be intolerant and adapt to its presence.

Be mindful that some candidates with disabilities such as dyslexia will find AI a useful tool.

Balancing AI assistance with personalisation to convey individual skills, knowledge and experience is key to leveraging AI benefits without compromising integrity.

During online interviews is there an initial question to the candidate to confirm via a verbal declaration that AI is not being used during the interview?

Real-time AI tools provide prompts or suggested answers during virtual interviews and candidates can appear more knowledgeable or competent than they are.

Consider a standard question to be asked at the outset of an online interview – is the candidate using any AI tools?

Are interviewers trained to spot red flags during online interviews that indicate the candidate is using AI?

Red flags include but are not limited to:

- Is the camera on?
- Do they have a second device/screen?
- Can you see their hands?
- Are they wearing an earpiece?
- Is the candidate engaged or distracted?
- Does the candidate mute and pause before answering?

Consider face to face interviews for senior or high-risk roles.

For further guidance: Guidance on the use of artificial intelligence in candidate applications | NHS Employers

Trusted family members, friends, and carers steal £51 million from pensioners

Report Fraud is run by the City of London Police and is the place to tell the police about economic crime outside of the NHS.

The organisation has recently reported that older and vulnerable people are seeing millions of pounds stolen from them with the fraud committed by those closest to them and is encouraging anyone who supports an elderly relative, acts under a power of attorney, is involved in administering an estate, or works within the care sector to remain vigilant for signs of financial abuse.

Data from Report Fraud reveals that criminals stole £93.8 million through fraud by abuse of position during the 2025/26 financial year, with people aged 70 and over accounting for more than £51 million of those losses. This type of fraud occurs when someone exploits a position of responsibility, authority, or trust to access and steal a victim's money, assets or property without lawful authority. Offenders are often family members, friends, carers, employees, or individuals entrusted to manage another person's finances or affairs.

The City of London Police has issued the following guidance:

- Review financial statements: check financial statements regularly for any unauthorised transactions. If anything appears suspicious, contact the bank as soon as possible.
- Watch for warning signs: be alert to unpaid bills, missing possessions, or unexpected changes to a will or bank account, as these may be indicators of financial abuse.

What to do if you are a victim of fraud by abuse of position:

- Tell your bank or card provider: if you notice any financial transactions made without lawful authority, notify your bank or card provider as soon as possible.
- Act quickly if something feels wrong: you can raise a safeguarding concern with your local authority's adult social care team. If a solicitor or deputy may be misusing their role, you can report your concerns to the Office of the Public Guardian.

What to do if You Suspect You Have Been a Victim of a Scam

If you receive a call and suspect it to be fraudulent, hang up. If you are suspicious about an email, forward it to:

- report@phishing.gov.uk
- If you are suspicious about a text message, forward it to the number 7726, which is free-of-charge.

If you believe you are the victim of a fraud, please report this to Report Fraud as soon as possible by visiting https://www.reportfraud.police.uk/ or calling **0300 123 2040**. Contact your bank immediately if you think you may have lost money.



Everyone has a part to play in fighting fraud. If you suspect any fraud, bribery or corruption against the NHS, contact your Anti-Crime Specialist.

Andrew Ede, Head of Investigations – Healthcare,
Email: andrew.ede1@nhs.net andrew.ede@tiaa.co.uk,
or fraud@tiaa.co.uk

You can also report via the NHS Counter Fraud Authority. You can call the anonymous, 24-hour reporting line on 0800 028 4060 or use the confidential online reporting form: Report NHS Fraud www.cfa.nhs.uk/reportfraud

tiaa.

Certified B Corporation
Learn more at bcorp.com

Disclaimer:
The content of this document is intended to give general information only. Its contents should not, therefore, be regarded as constituting specific advice, and should not be relied on as such. No specific action should be taken without seeking appropriate professional advice.

tiaa.co.uk
T: 0845 300 3333