tiaa

FRAUD STOP

Healthcare
Spring 2023

CASES IN COURT

Details of prosecutions involving healthcare workers and suppliers

→ SEE PAGE 2

SCAM ALERTS

Current scams in circulation that can target anyone

→ SEE PAGE 3

FRAUD ALERTS

What other frauds are targeting healthcare organisations?

→ SEE PAGE 4

Introduction

The National Crime Agency website states that fraud is the most commonly experienced crime in the UK and costs the UK many billions of pounds every year. The impact of fraud can be devastating to individuals and organisations.

Fraud is deception carried out for personal gain, usually money. The NHS Counter Fraud Authority estimates that the NHS is vulnerable to nearly £1.2 billion worth of fraud each year.

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

This edition covers NHS staff and suppliers who have been prosecuted, other common frauds targeting the healthcare sector, and common scams in circulation.

Cases in Court: Three men guilty of Theft, Fraud and Bribery Act Offences against the NHS

In March 2023 at Crown Court, two men were found guilty of Theft, Fraud and Bribery Act offences against the NHS following a seven-week trial. A third man had entered a guilty plea prior to the trial commencing. The investigation was undertaken by the NHS Counter Fraud Authority (NHSCFA), with the prosecution led by the Crown Prosecution Service (CPS), with the total value of all offences being more than £600,000.

A former Theatre Manager was found guilty of offences under the Theft, Fraud and Bribery Acts. He was remanded in custody to be sentenced on Wednesday 24th May.

A Chief Executive Officer of a company that had supplied medical equipment to the NHS was found guilty of one charge of bribing the Theatre Manager. A Director of a second NHS supplier had already pleaded guilty to one charge of bribing the Theatre Manager prior to the trial opening.

The Court heard that the Theatre Manager was in a position of responsibility within the NHS, where he was able to procure medical equipment on behalf of the NHS Trust. As part of his role, he was required to make purchase order requests for items required for surgical procedures carried out within the hospital. The investigation undertaken by the NHSCFA was able to prove that he was in a relationship with the two Trust suppliers in which he accepted bribes to ensure that the Trust procured medical equipment from the companies concerned. The Theatre Manager was also convicted of receiving payments from two further suppliers to the NHS Trust. He ordered goods from these companies that he himself had supplied to them. In return, he received at least two-thirds of the value of the goods invoiced.

During the investigation the Theatre Manager's house was searched, and a large number of orthopaedic implantable devices, surgical instruments and medical equipment with a value in excess of £65K was recovered. The investigation was able to prove that these had been stolen from the Trust. All three will be sentenced at Crown Court at a later date after which the NHSCFA and the CPS will be leading a process under the Proceeds of Crime Act aiming to recover any funds fraudulently obtained back to the NHS.

More information at: https://cfa.nhs.uk/about-nhscfa/latest-news/Two-men-found-guilty-of-fraud-and-bribery

Fake doctor sentenced to seven years for fraud and forgery

A woman who forged her medical qualifications to obtain senior positions within the NHS as a hospital Psychiatrist has been sentenced to seven years at Crown Court after being found guilty of 20 offences including fraud and forgery.

In an investigation led by the Police and supported by the NHS Counter Fraud Authority, the fake doctor was found to have fraudulently obtained in excess of £1million from the NHS during the twenty-two years that she worked within a number of UK health bodies posing as a qualified psychiatrist.

In 1995, she presented to the General Medical Council (GMC) supplying documents and information in support of her application to obtain UK doctor registration. These documents included a degree certificate from overseas, and a letter written by the faculty registrar confirming her qualifications. Investigations subsequently revealed that this documentation was completely false, and she had subsequently secured positions in a number of NHS bodies within the UK over the course of the next 22 years – all of which were based on her false and forged qualifications.

Specialist financial investigators have worked to identify and restrain assets owned by the fake doctor and will now use their powers under the Proceeds of Crime Act to ensure that money defrauded by her is returned to the NHS for patient care.

More information at: https://cfa.nhs.uk/about-nhscfa/latest-news/fake-doctor-sentenced-to-seven-years

Scam alerts - Criminals are targeting WhatsApp users by posing as a friend and asking for a security code.

In a variance of a previous WhatsApp scam, Action Fraud is reporting a scam that steals access to a WhatsApp user's account. The scam begins when a criminal gets access to another WhatsApp account which has you listed as a contact. The criminal, posing as your friend or someone that is a member of a WhatsApp group you are in, will then send you seemingly normal messages to try and start a conversation with you.

However, around the same time you will receive a text message from WhatsApp with a six-digit code. This is because the criminal has been trying to login to WhatsApp using your mobile number. The criminal will claim that they sent you their code by accident and ask you to help them by sending it to them. Once the criminal has this code, they can login to your WhatsApp account and lock you out. The criminal will then use the same tactic with your WhatsApp contacts in an effort to steal more accounts and use them to perpetrate fraud.

ADVICE FROM ACTION FRAUD IS TO:

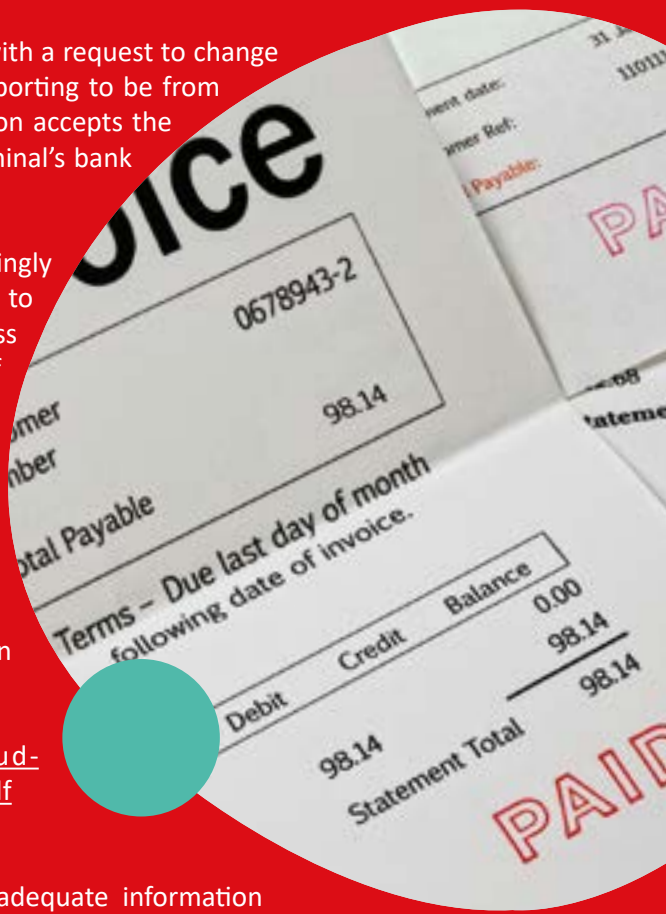
- **Set up two-step verification to give an extra layer of protection to your account: Tap Settings > Account >Two-step verification > Enable.**
- **THINK. CALL. If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity.**
- **Never share your account's activation code (that is the 6 digit code you receive via SMS)**
- **You can report spam messages or block a sender within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions.**

(https://www.actionfraud.police.uk/alert/warning-issued-to-whatsapp-users-over-account-takeover-scam)

Mandate fraud

Mandate fraud occurs when someone contacts an organisation with a request to change a direct debit, standing order or bank transfer mandate, by purporting to be from a genuine supplier that payments are made to. If the organisation accepts the fraudulent request, the payments are then diverted into the criminal's bank account.

NHS organisations are continuing to be victims of increasingly sophisticated mandate frauds. A TIAA ICB client came very close to losing nearly 200K recently. Fraudsters hacked into an email address of a Director of a supplier and communicated with ICB finance staff regarding a change of bank account and the provision of a phone number for the security checks to be completed. When the fraudsters realised that they would need supplier information for the security checks, they then created a fake NHS domain and communicated with the supplier for the requested information, purporting to be ICB finance staff.



The NHS Counter Fraud Authority has updated their guidance on mandate fraud prevention as follows:

https://cfa.nhs.uk/resources/downloads/guidance/fraud-awareness/quick-reference-guides/mandate-fraud-quick-guide.pdf

Action Point
Any supplier conducting business with the NHS should have adequate information governance and comply with the requirements of the NHS Data Security and Protection Toolkit – does your organisation receive assurance on this from suppliers?

Fake positive covid test results

A TIAA Anti-Crime Specialist has conducted a number of investigations where NHS staff have provided fake positive covid test results, leading to the staff being dismissed, salary repaid for false sickness absence and referred to their regulatory bodies if relevant. Here are just a couple of images of the 'positive' tests supplied to support time off sick.

There is no serial number on this test – it has been obtained from google images!

This image clearly has two drawn on lies purportedly showing a positive result!

Action Point

Line Managers should scrutinise images of test results and discuss any concerns with their Anti-Crime Specialist.

Overlapping Shifts

Healthcare staff working overlapping shifts has become increasingly more prevalent since the pandemic. Intelligence suggests that the increase in remote working can cause staff to become disconnected from their employer which subsequently increases the opportunity for staff to undertake overlapping employment. Whilst an employer may not object to staff working a second job, it should not conflict with their primary employment or adversely impact either employer.

TIAA has observed an increase in the number of referrals received where duplicate or overlapping employment is the key factor. A recent investigation concerned an individual who had two laptops for two separate Trusts, open on a desk at the same time. These matters have been difficult to prove to a criminal standard because of weaknesses in the organisation's governance and/or remote working procedures.

Action Point

Remedial recommendations are that the organisation provides clear guidance to staff on its expectations regarding secondary employment.

If you suspect any fraud, bribery or corruption against a healthcare organisation, contact your Anti-Crime Specialist.

- **Melanie Alflatt, Director - Risk and Advisory, Email:** fraud@tiaa.co.uk
- **Alternatively, call** the 24-hour reporting line on **0800 028 4060** or use the online reporting form: Report NHS fraud | Help fight fraud within the NHS | Report your fraud concerns and suspicions using a confidential online form (cfa.nhs.uk). All reports are treated in confidence and you have the option to remain anonymous.