NOTICE FRAUD: WINTER 2024

Welcome to the RSM NHS counter fraud newsletter, providing insights into current fraud trends and risks, our counter fraud work, and recent fraud cases.

Conflict of Interest

A conflict of interest occurs where your personal affiliations or previous employment affects, or is perceived to affect, the decisions you make in your current role. This is usually because you have a personal link with an organisation that does business with your employer or may do in the future.

Declarations of interest are sought from staff, as a vital step in NHS governance that ensures transparency in decision making. Appropriate management of conflict of interests is also key to fostering a strong anti-fraud and bribery culture.

Types of interest – key considerations

- Actual or potential: Does the conflict exist already, eg you own a business supplying goods or services to the NHS, or could your business be a supplier in the future?
- Direct or indirect: Is the business owned by you, or by a close friend or family member?
- Professional or personal: Would the interest provide financial benefit, or enhance your professional reputation? Does it benefit your interests outside of work?

What can you do

- Understand your responsibilities for your role and reporting mechanisms and deadlines, check your organisation's intranet and declaration of interest policy. Organisations often require senior staff to make a declaration even if they have no interests to declare. This is known as a 'Nil' declaration.
- Report all your interests promptly. NHS England guidance states that all interests should be declared 'as soon as circumstances change, and new interests arise'.

What should you declare

- Received gifts or hospitality from suppliers or contractors, or high value items from patients. Undeclared receipts can create the impression of bias in decision making.
- Additional employment or clinical private practice. It can create a conflict for your time, even if it is unrelated to your NHS role.
- If you own/run a business/charity, are a director/trustee of one, or have controlling shares in a publicly listed or private company, including those owned by close friends or relatives, it can create a conflict of interest.

If you are unsure, obtain additional guidance from your organisation's governance team. If in doubt, declare.

CONCEALED SECONDARY EMPLOYMENT AND FALSIFIED SICK LEAVE CLAIMS

In August 2023, Bridgitte Magno, an NHS nurse pleaded guilty to fraud offences. She defrauded the NHS of £2,587. With the fraud perpetrated against a public body, and the likelihood of reoffending, Magno received a custodial sentence of 20 weeks, suspended for 24 months. She was ordered to pay compensation to the Trust to the value of the monies defrauded.

Magno failed to declare secondary employment at a medical staffing agency. She had been refused a period of leave, for which she subsequently claimed to be sick. The Trust investigated, identifying four periods over 12 months where Magno had taken four to six weeks off with paid sick leave whilst working elsewhere in similar roles.

KEEPING YOU UP TO DATE

By raising awareness of fraud risks, we aim to protect NHS staff and resources.

Upcoming fraud awareness sessions

Recruitment and ID verification

Our recent interactive recruitment session received excellent feedback from the 154 attendees across 23 NHS organisations. We encourage staff to take advantage of our training sessions which cover identity documents, qualifications and references, and are delivered by RSM staff that have previously worked at the Home Office and Passport Office.

Session date and time: 7 March 2024 10am – 1pm

Please click here to register for the next Fraud, Bribery and ID Verification Awareness Session.

Cyber fraud and data security

Cyber fraud and security are crucial issues, as NHS organisations face more frequent and complex attacks. Our quarterly sessions are raising staff awareness of the risks of cyber enabled fraud, data theft and wider cyber security issues.

Our sessions provide information on the types of attacks we see, and how to identify and prevent cyber fraud to protect NHS resources. We also cover common scams that target individuals in their personal lives.

Session date and time: 30 January 2024 10 – 11:30am

Please click here to register for our interactive Cyber Fraud Awareness session.

Watch out for QR code scams in car parks

Reports to the consumer service Which highlights an increasing trend in QR code scams. Data from Action Fraud reveals that the number of QR scams up to September 2023 was 411, compared to 380 in 2022, and 291 in 2021.

Fraudsters are placing false QR codes on ticket machines in car parks. Genuine codes allow you to pay for parking easily, but fake codes lead you to a fraudulent website that harvests your card payment details. If you fall victim to this scam, you may also incur a fine for failing to pay for your parking.

A November 2023 BBC article highlighted how one victim lost £13,000 after using a fake QR code at a railway station. The scammers used information from the fake parking website and social engineering techniques to pose as the victim's bank.

After gaining access to the accounts, fraudsters changed the victim's email address, received duplicates of her cards and took out a loan in their name for £7,500.

To access training or report a fraud you should contact your Local Counter Fraud Specialist (LCFS) directly:

T: 0121 214 3149

E: manjit.sandhu@rsmuk.com

You can also report fraud anonymously on 0800 028 4060, or online via https://cfa.nhs.uk/reportfraud