Fraud Awareness Newsletter

Local Counter Fraud Specialists (LCFS) | 2018/19 Q3

Welcome to this edition of the Fraud Awareness Newsletter. We will provide an update on the latest NHS fraud cases. While the majority of people who work in or use the NHS are honest, fraud does exist and is a serious issue.
Fraud in the NHS diverts resources away from patient care, salaries and services. Your LCFS team aims to make people aware that fraud is being tackled.

Swansea dentist sentenced for NHS fraud

Following an investigation by the NHS Counter Fraud Service Wales, Elizabeth Anne White pleaded guilty to fraud against the NHS.

The dentist defrauded ABM University Health Board of over £30,000 when she was the co-owner of Morgan and White Dental practice. She paid back the entire amount before receiving a 12 month sentence.

White made 398 false claims for Units of Dental Activity, relating to dental treatment between 2006 and 2014, including 315 instances of multiple claims by "treatment splitting" and 83 bogus claims for examinations or treatment which was not provided.

Investigators spotted reminders on patient records to enter false treatment dates on the related claim forms.

Karl Bishop, ABM University Health Board Dental Director, said: *"By defrauding the NHS in this way, she not only abused her privileged position of trust, but took funds for herself which should have been used for patients."*

NHS CFS Wales' lead investigator on the case, Mark Weston, added: *"The ABM University Health Board can now spend the recovered £34,395.09 on delivering NHS services."*

The Morgan and White practice has been sold and is under new ownership.

Source: NHSCFA, October 2018

INTERNATIONAL
FRAUD AWARENESS WEEK
November 11-17, 2018

HOSPITAL IT Manager sentenced for selling NHS iPhones

Peter Summerhill, 35, of Middleborough, profited from selling 18 iPhone handsets while working in his senior position at the County Durham and Darlington NHS Foundation Trust.

The fraud was uncovered after Summerhill, who has now been sacked from his job, attempted to sell some of the phones through website Mazuma Mobile.

Mazuma contacted Vodafone to find out who the phones belonged to.

The Trust issues some staff, including community midwives, nurses, and on-call clinical staff, with iPhones necessary to carry out their job. But Summerhill is understood to have been ordering in more phones than necessary, then selling both new and used handsets.

Summerhill pleaded guilty to fraud while compromising his position of trust, over the period from December 2016 to November 2017. When he appeared before magistrates in September 2018, the value of the fraud was £10,706.

He was sentenced to four months in prison and ordered to pay a victim surcharge of £115 and costs of £85.

A spokesperson for County Durham and Darlington NHS Foundation Trust said: *"A former senior member of our IT team abused his position of responsibility and the trust placed in him by selling new and used mobile phones belonging to the Trust, for personal gain."*

Source: The Northern Echo, September 2018

What is Mandate Fraud?

Mandate fraud occurs when someone gets an organisation to change a direct debit, standing order or bank transfer mandate. This is often someone pretending to be a current supplier and getting an organisation to make unauthorised regular payments to the fraudster.

Case study:
The shared services provider who dealt with the financial services in an NHS health body received a fax from a construction company with whom they had a contract. The health body believe that the criminals obtained their information from material available publicly, such as publicised invoices and press releases. An £897,000 interim payment was agreed to the contractor and subsequently paid. The bank managed to trace some of the funds into overseas banks and £537,000 was returned to the Trust a few days later. This left a £360,000 shortfall, money earmarked for patient care. The Trust has since adopted NHSCFA's guidance and improved their systems.

Here are some examples of what you can do to help prevent mandate fraud:

- Always verify requests to change supplier details by using contact details already held on file
- If a call from a supplier seems suspicious, hang up and call back using established contact details
- Be aware of "social engineering" techniques: look out for urgent requests to change details, lack of supplier logo or address
- Suppliers should periodically be asked to confirm information already held by the health body
- Ensure clear written instructions and procedures for all staff involved, detailing access levels and responsibilities

NHS fraud.
Spot it. Report it.
Together we stop it.

For further information:
https://cfa.nhs.uk/resources/downloads/guidance/NHSCFA%20Invoice%20fraud%20guidance%20-%20v1.0%20July%202018.pdf

Meet your counter fraud team

Contact your local counter fraud specialist team in absolute confidence: *"We're here to talk about any concerns you may have about fraud and corruption, or just happy to discuss why fraud is a big issue for the NHS. Never be afraid to give us a call."*

Neil Mohan
T: 07843 325993
E: neil.mohan@nhs.net

Tasnim Putwa
M: 07739 875923
E: tasnim.putwa@nhs.net