LCFS NEWSLETTER

Your counter fraud service — January 2015

In this issue

Special points of interest:

- Contact details for your LCFS
- The NHS fraud and corruption reporting line

Please report any concerns or suspicions you may have. You will be helping to protect NHS funds.

Counter Fraud Survey 2015

Fraud is a hidden crime that effects all organisations including the NHS. We have devised a questionnaire that has been designed to assess your understanding of fraud and bribery, and the effectiveness of the counter fraud and bribery arrangements which exist within the Trust.

The questionnaire can be accessed via the link recently provided by the Southend CCG Communications Team. There are 10 questions and it should take less than 5 minutes to complete.

You are welcome to keep your response anonymous; but if you chose to identify your any comments you do make will be treated in strictest confidence and will not be disclosed to the Southend CCG.

Practice Manager sentenced for selling free NHS treatment

A practice manager, from Birmingham, who accepted money to register "patients" at a health centre has been sentenced to two years' imprisonment and suspended for 12 months, following an investigation by NHS Protect.

Asif Butt, 53, pleaded guilty to Fraud contrary to the Fraud Act 2006, at Birmingham Crown Court on 19th December 2014. He must also complete 200 hours' of unpaid work and will be subject to a 12 month supervision order.

Butt was exposed when he was filmed by an undercover BBC reporter and appeared on Panorama in October 2012. He accepted payments to register the names of six "patients" at the Sparkbrook Health and Community Centre. One of these "patients" was the undercover reporter, who went on to receive a free MRI scan as a result.

Richard Rippin, Head of Operations at NHS Protect, said, "Asif Butt deliberately abused his position of trust within the NHS in order to make a personal financial gain. All allegations of fraud reported to NHS Protect are given full consideration and, wherever it is appropriate to do so, we will seek to prosecute offenders".

£229,000 Procurement Fraud

Two NHS managers, who masterminded a 5-year procurement fraud worth £229,000 against a health authority in the North West, were jailed for over five years in total at Manchester Crown Court on 27th November 2014.

John Leigh, 54, and Deborah Hancox, 44, pleaded guilty to conspiracy to defraud the NHS. Leigh also pleaded guilty to conspiracy to conceal criminal property. The couple were arrested in December 2013 in Cyprus and extradited to the UK having fled the country in 2009.

The systematic fraud took place between 2003 and 2008. Leigh and Hancox both worked at the North Western Deanery, part of the North West Strategic Health Authority. Leigh was employed as an IT Network Manager and Hancox as an Information and Quality Assurance Manager. They lived a comfortable lifestyle, buying a cottage in the Lake District, driving a Jaguar 4.2 V8 Convertible, and investing hundreds of thousands of pounds in Iraq, the United Arab Emirates and Turkey.

The pair used three companies as a front to disguise their ongoing fraud – Action Technology Ltd, Bibi's IT Solutions Ltd and Wiscom Technology Ltd. These companies sold IT equipment to the North Western Deanery at inflated prices – their combined fraudulent turnover was more than £1million. Leigh and Hancox had links to all of them, but neither made any declaration of interest to the health authority.

Following an anonymous tip off, the matter was investigated by a Local Counter Fraud Specialist (LCFS), before being referred to NHS Protect, whose fraud investigators worked closely with Greater Manchester Police to secure a successful result. They also worked with the National Crime Agency to issue European Arrest Warrants and to have the fugitives extradited back to the UK.

Sue Frith, Managing Director of NHS Protect, said, "This was a serious fraud against the NHS, cynically carried out by two individuals abusing their positions of trust and authority. Their determined attempts to evade justice compound the crimes. All suspicions of fraud reported to NHS Protect will be followed up, and investigated wherever appropriate. We press for prosecution of offenders and seek the strongest possible sanctions, so public money is not diverted from patient care".

Police Sergeant Laura Walters said: "This couple were involved in a well-orchestrated and meticulously planned conspiracy to defraud the NHS out of hundreds of thousands of pounds. I am delighted this case has finally been concluded and these con artists have been exposed and brought to justice."

Invoice Fraud

Invoice Fraud happens when a company or organisation is tricked into changing bank account payee details for a sizeable payment. Criminals pose as regular suppliers to the company or organisation and will make a formal request for bank account details to be changed.

Fraudsters make contact with the organisations finance teams, posing as suppliers. Payments are made to them and the fraud is often only discovered when the legitimate supplier chases for non-payment. At that point recovery of the funds lost is very difficult.

Following some of these simple steps will protect against invoice fraud:

- Ensure that all staff who process supplier invoices and who have the authority to change bank details are vigilant. They should always double check changes to supplier names, addresses and changes to invoiced amounts.
- Establish a designated point of contact with suppliers to whom your company or organisation makes regular payments. Raise all invoice issues and concerns with this person.
- Check the Logos. Logos on counterfeit invoices are often blurred and these invoices often contain account details to which the payment should be made.

Every organisation is vulnerable to Invoice Fraud. The vigilance of every member of staff within an organisation is the key to prevention.

Telephone Fraud

Telephone fraud is being used increasingly by criminals to deceive organisations into revealing financial information or to encourage the transfer of funds into a bank account held by the criminal. This type of fraud is known as ‘Vishing’.

Posing as a supplier, a police officer, or bank staff, criminals will make an attempt to obtain bank account details or will ask for bank payee details to be altered so regular payments normally transferred to a genuine supplier account are instead made into their own account.

A variation of this fraud involves the criminal posing as a senior bank official or police officer investigating internal fraud at your company bank. They will try to persuade a member of staff that in order to protect your organisation’s fund, all money must be transferred to a ‘secure’ account. They are advised not to give the bank a reason for the transfer in case the teller is involved in the internal fraud. Remember:

- Do not assume that every telephone call is an honest one. Criminals may already have enough information about your company to appear genuine.
- Be wary of requests for financial information and alterations to bank transfers.
- If you are suspicious, do not be afraid to terminate the call.
- Remember that caller display IDs can be manipulated to disguise the origin of the call. If in doubt, call back using an independently verified number.

Should you have any concerns regarding vishing then please contact the Local Counter Fraud Specialist, our details are at the end of this newsletter.

Whistleblowing

Whistleblowing is when an employee reports any suspected wrongdoing at work. This can occur from anything that is suspected as being illegal, failing to follow the correct rules and procedures in the workplace or of any negligence and/or abuse of the suspected individual with regards to their position of responsibility. The CCG has a whistleblowing policy which you can refer to for additional information.

Whistleblowing is encouraged as it ensures the protection and anonymity of the individual who has raises suspicion of any instances of fraud in the workplace. In the event of any investigations currently under review, the individual suspected will not be aware of the whistleblower ensuring the safeguarding of all employees within the workplace. All allegations made either via the whistle-blowing policy or through the fraud line are taken seriously and will be investigated thoroughly.

Fraud! See it, Report it, Stop it.

Contact your Local Counter Fraud Specialist (LCFS)

Your Local Counter Fraud Specialists

Brendan Harper LCFS

Tel: 07917 790 112

brendan.harper@mazars.co.uk or

brendan.harper@nhs.net

Shelly Rai LCFS

Tel: 0778 830 1124

Shelly.Rai@mazars.co.uk or

Shelly.Rai@nhs.net

Report NHS fraud
0800 028 40 60
NHS Protect