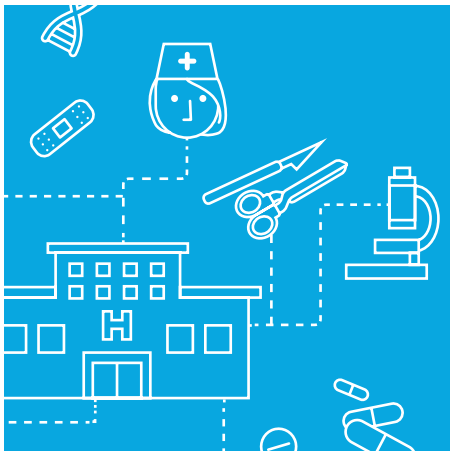
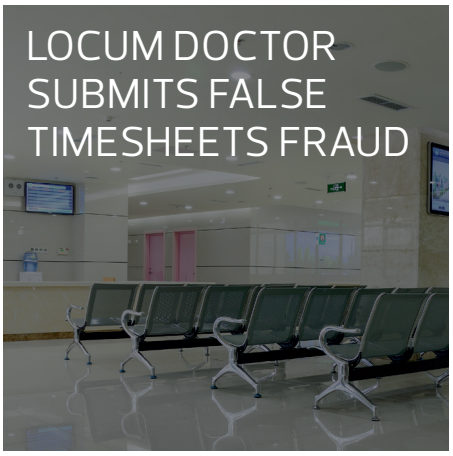
DECEMBER 2016





FIVE YEAR MASTERMIND PROCUREMENT FRAUD

NOTICE FRAUD

This edition of Notice Fraud is designed to bring recent cases or emerging scams to your attention to help you recognise the signs of fraud in the NHS.

SENIOR COMMISSIONING MANAGER JAILED FOR £145K INVOICE FRAUD

The subject was contracted via an agency (which played no part in his crimes) for the position of senior commissioning manager. Within this role the subject was responsible for the approval and management of funding for mental health "cost per case" care packages for patients with learning difficulties.

The investigation began after the clinical commissioning group (CCG) identified a suspicious invoice from a provider. The invoice related to a patient whom the subject had previously advised had been discharged (and therefore not incurring these costs). The provider was found to be registered to the subject's home address and a former address.

The investigation uncovered links between the subject and a second provider who was also invoicing the CCG for delivery of care packages. The invoices from the two providers totaled £144,986.60 for services that were never delivered. The payments were paid into a bank account actually owned by the subject.

The investigation established that the subject had a sign off limit of £10,000 and all of the invoices from the two providers were just under that amount, so the subject could authorise them.

The subject was convicted of Fraud by Abuse of Position, contrary to Section 3 of the Fraud Act 2006 and jailed for two years and three months. The sentencing judge took account of the fact that the subject had paid back £93,681 to the CCG.

FIVE YEAR MASTERMIND PROCUREMENT FRAUD

Two NHS managers masterminded a procurement fraud by failing to declare interests in three IT companies who sold IT equipment to the North Western Deanery at inflated prices.

Their fraud took place between 2003 and 2008, when the subjects' both worked at the North Western Deanery, at the time part of the North West Strategic Health Authority.

The first subject was sentenced to 44 months' imprisonment for conspiracy to defraud the NHS and to 40 months for conspiracy to conceal criminal property – to run concurrently. If the subject does not pay £177,999.84 within three months, he will face a default jail sentence of six months.

The second subject was sentenced to two years' imprisonment for conspiracy to defraud the NHS. If the subject does not pay £6,930.34 within three months, her default jail sentence will be two months.

LOCUM DOCTOR SUBMITS FALSE TIMESHEETS FRAUD

Over a two month period, a locum doctor claimed to provide NHS orthopaedic services, for work he never undertook, whilst under an employment agency contract to a foundation Trust. The subject forged the signatures of three consultants on timesheets to support his false claims. The value of the fraud totalled £13k.

The subject was sentenced to eight months imprisonment and was to be subject of a General Medical Council panel to review his professional ability to practice. The subject is also facing a hearing to recover the monies defrauded from the NHS from his personal assets. This hearing will take place in January 2017.

DOCTORS' CVS FOUND ONLINE

Full CVs of two doctors from a Mental Health Trust were found online. The CVs were made available online through a charitable foundation, and were accessible through a Google Search.

The CVs contained the doctors' personal details including dates of birth, home addresses and personal contact details. These could obviously be used by patients seeking to locate the doctors, or by fraudsters seeking to use their identity to create credit accounts to steal money.

We have been able to get the CVs removed and replaced with redacted versions. You should regularly conduct internet searches on yourself to ascertain what information is publicly available. Your LCFS can assist in seeking the removal of sensitive data.

CHIEF EXECUTIVE OFFICER SCAM

Be aware of emails containing urgent payment requests from senior members of staff such as the director of finance or the chief executive. The email is accompanied with payment instructions to a specific account. The email is a targeted phishing scam which is enabled through gaining access to senior members email accounts or emails sent through a recently registered domain name which is very similar to the organisations email address.

'TIS THE SEASON TO BE JOLLY'

With Christmas just around the corner, everything tends to get hectic. It can be easy, with so much Christmas cheer around, to forget about the darker side of Christmas; in particular fraud. Below is some practical advice to help protect you:

- Be suspicious of all 'Too good to be true' offers and deals.
- Do not agree to offers and deals immediately. Insist on time to reflect and seek advice before making any decisions.
- Do not hand over money or sign anything until you have checked the credentials of the company/ individual.
- Never send money to anyone you do not know or trust (whether in the UK or abroad) or use methods of payment you are not comfortable with.
- Never give banking or personal details to anyone you do not know or trust. This information is valuable. Make sure you protect it.
- Always log on to a website via a trusted search engine rather than clicking on links provided in an email.
- Do not be embarrassed to report a scam. Scammers are cunning and clever; there is no shame in being deceived. By reporting you will make it more difficult for them to deceive others.

REPORTING CONCERNS

If you have suspicions that fraud may be occurring or wish to receive further information about the above please contact your Local Counter Fraud Specialist (LCFS).

Alternatively you can report any concerns to NHS Protect on 0800 028 40 60 (between 8am and 5pm, Monday to Friday) or via the online reporting form: **http://www.reportnhsfraud.nhs.uk/**.
All information provided via this secure website is completely confidential.

It is the LCFS's role to take every allegation of fraud or bribery seriously and to provide anonymity and confidentiality for anyone who reports a concern. It is recommended that you refer to the organisations policy on fraud when reporting allegations for further information on how you are protected.

rsmuk.com