



# COUNTERING FRAUD AND BRIBERY IN NHS OXFORDSHIRE CLINICAL COMMISSIONING GROUP

What you need to know

THE POWER OF BEING UNDERSTOOD  
AUDIT | TAX | CONSULTING



---

# INTRODUCTIONS

I am the Local Counter Fraud Specialist (LCFS) at NHS Oxfordshire Clinical Commissioning Group (the CCG) and wanted to take this opportunity to formally introduce myself.

We all recognise that fraud is a growing threat both internally and externally. The CCG is dedicated to reducing the level of fraud to an absolute minimum and to taking action against those who have committed fraud.

This pack has been prepared to help raise awareness of fraud to help you recognise it, how to report it and to look at ways to help prevent it.

In order to achieve greater awareness and assist with training I am happy to meet with individual staff members, attend team meetings, conduct workshops and deliver awareness presentations.

Additional material is provided on the counter fraud pages on the intranet. Please take some time to have a look.

**Erin Sims**

**Local Counter Fraud Specialist (LCFS)**

**NHS Oxfordshire Clinical Commissioning Group**



The CCG is dedicated to reducing the level of fraud and bribery to a minimum and taking action against those who have committed fraud. There is material available on our intranet pages to help raise awareness and education of fraud within the NHS to help recognise it; report it; and help prevent it. We have a team of Counter Fraud Specialists who are happy to meet with individual staff members; attend team meetings; conduct workshops; and deliver awareness presentations.

If you have any concerns in relation to fraud or bribery at Oxfordshire CCG, or would like to know more, please take the time to view the Counter Fraud and Bribery policy, Counter Fraud intranet pages or contact Erin Sims directly. Alternatively, you can report concerns anonymously to the NHS Fraud and Corruption Reporting Line 0800 028 40 60 or online at <https://cfa.nhs.uk/reportfraud>.

**Gareth Kenworthy, Director of Finance, NHS Oxfordshire Clinical Commissioning Group**

---

# THE ROLE OF THE LOCAL COUNTER FRAUD SPECIALIST

There are four areas to my role

## Strategic governance

Reporting to and liaising with the Executives, Non-Executives and the Audit Committee

## Inform and involve

Raising awareness of the counter fraud provision within the CCG

## Prevent and deter

Reviewing and testing current policies and procedures with a view to strengthening them and reducing the risk of fraud and bribery

## Hold to account

Conducting criminal investigations as a result of referrals received from staff or from findings as a result of one of my prevent and deter exercises.

---

## POLICIES AND PROCEDURES

One of the methods used to prevent fraud and bribery is to have clearly defined policies and procedures in place.

Policies and procedures go hand in hand to clarify:

- how the CCG wants to conduct its services;
- what levels of authority are required for decisions;
- the steps to take;
- which forms or documents to use; and
- what processes will be undertaken when things go wrong.

Policies and procedures are regularly reviewed to ensure they are accurate and compliant. The current versions can be found on the CCG intranet.

Some of the policies relevant to the prevention of fraud and bribery at the CCG are:



---

# WHAT IS FRAUD?

---

Fraud can be defined as:

A person acting dishonestly with the intent of making a gain for themselves or anyone else, or inflicting a loss (or a risk of loss) on another.

There are three main offences of fraud:

## False representation

This is the most common type of fraud investigated within the NHS. It normally involves a false declaration being made, such as informing your line manager that you are unable to work due to sickness, and being paid sick pay from the CCG, but then being paid for secondary employment too, whether that is in the NHS or otherwise.

## Failure to disclose

This could be relating to any information where there is a legal duty to disclose information. For example, failing to disclose a criminal record or anything that could affect your DBS checks.

## Abuse of position

This is when someone abuses their position of authority, for personal or financial gain, or to cause loss to another. Essentially, those who know how to use the systems, but ultimately abuse them too. For example, a member of the payroll team adding family members to the payroll system.

---

# EXAMPLES OF FRAUDS COMMITTED AGAINST CLINICAL COMMISSIONING GROUPS

**The recurrent frauds are (of which this list is not an exhaustive list).**

- Payroll fraud - (payments made to fictitious employees or fraudulent manipulation of payment; false or inflated travel, expense claims, timesheet fraud claiming for hours that have not been worked or submitting duplicate timesheets).
- Fraudulent job applications (e.g. false or misrepresentation of qualifications / experience or immigration status).
- Patient fraud (e.g. false travel claims, fraudulently claiming exemptions from pharmaceutical charges, amending prescriptions to gain additional medicine and multi registrations).
- Submission of false / inflated and duplicate invoices for goods or services.
- Emails sent to senior members of staff requesting urgent payments.
- Procurement fraud (e.g. bribes manipulating the tender process, splitting contracts, price fixing and collusion between employees and contractors).
- Failing to declare interests / hospitality (particularly relating to procurement / commissioning).
- Pharmaceutical fraud by companies (e.g. overcharging for drugs, supplying inferior or reduced quantities of drugs).
- Primary care contractors (e.g. creation of ghost patients, claiming for services not provided or claims for NHS allowances for individuals who are not entitled).

There is no one type of fraud nor one type of person who commits fraud. By ensuring that we all understand what NHS fraud may look like, we increase the chances of reducing the threat instead of feeling the effects.

---

# PROCUREMENT FRAUD

---

Recent publications have estimated the level of procurement fraud in the NHS in 2017 is anywhere between £1.7bn (Annual Fraud Indicator Review 2017, UK Fraud Costs Measurement Committee) and £252m (Operational Strategy 2017-2020, NHS Counter Fraud Authority).

Whilst the methodologies behind these estimates may differ, it is clear procurement fraud is deemed to be a key fraud risk for the NHS.

Procurement fraud is any fraud that relates to an organisation purchasing goods or commissioning services from third parties. Fraud can occur at two stages of the procurement lifecycle: pre-contract award and post-contract award.

Fraud occurring at the pre-contract award phase normally involves a lack of compliance with policies, accompanied by acts of collusion and corruption. This can include:

- eliminating or reducing competition through the use of tender waivers, extending contracts without consideration of a competitive process and influencing procurement specifications;
- favouring of suppliers by providing insider information and biased evaluation process including marking of the bids; and
- non-delivery of the terms of the contract specification, changes to contracts to favour the supplier and extension of contract to benefit the supplier.

The post-contract stage tends to involve overpayments to contractors, through false or duplicating invoicing, and payments for substandard work, or work not completed.

## **Locksmith used his position to defraud a NHS trust out of £600,000.**

The locksmith was employed at an NHS trust as their permanent locksmith. His duties included obtaining best value quotes for locksmith suppliers. The locksmith purchased materials from his own company to supply materials to the trust. The purchases were up to 1,200 per cent over market rates.

The locksmith was jailed for six years.

## **Two NHS managers masterminded a five-year procurement fraud worth £229,000.**

The pair created a number of companies, as a front to disguise their fraud and sold IT equipment at inflated prices. Fraudulent turnover was estimated to be over £1m.

The fraudsters were subsequently jailed for over five years.

---

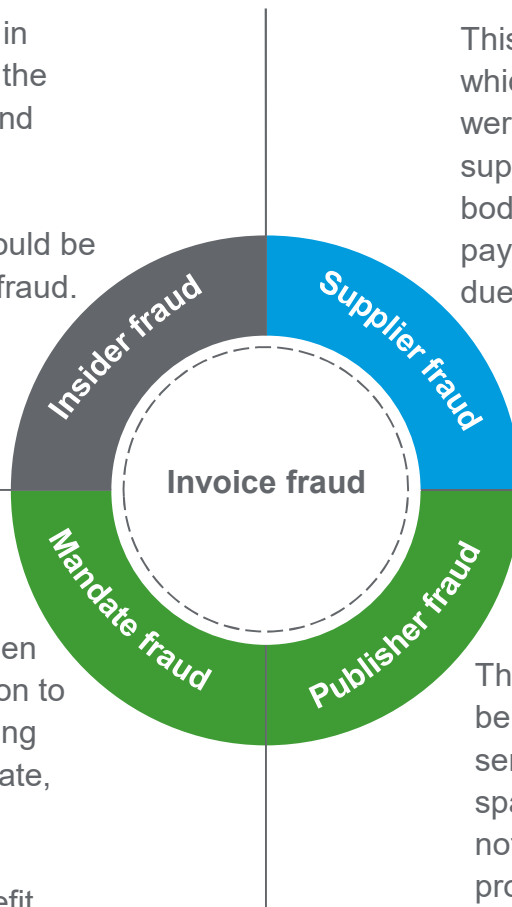
# INVOICE FRAUD

---

## There are four common kinds of invoice fraud

This refers to cases of fraud in which an insider's access to the NHS organisation's assets and payments, or their ability to influence the outcomes of organisational processes, would be essential for committing the fraud.

This includes any fraud for which it can be shown that steps were deliberately taken by the supplier to mislead a health body with a view to obtaining payments that were not properly due.



This type of fraud occurs when someone gets an organisation to change a direct debit, standing order or bank transfer mandate, by purporting to be from a supplier they make regular payments to in order to benefit from unauthorised payments.

This involves health bodies being misled into paying for services such as advertising space in publications, which are not required and may not be provided.

### 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 organisation's email address.

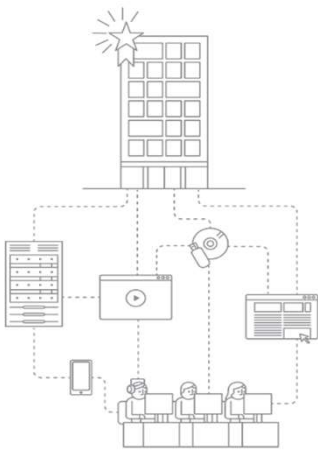


---

# CYBER FRAUD

---

Much of today's fraud is committed with the use of computers. It is easy for fraudsters to copy legitimate websites to try to trick you in to handing over personal or sensitive information. The WannaCry cyber attack which affected 47 NHS Trusts was started by an employee opening a link in an email.



- **Be cautious** of any unfamiliar emails or unusual requests. Check the details of the sender by hovering your mouse over the sender's email address.
- If in doubt **don't click**.
- Contact the sender using alternative details and confirm that they have sent you the attachments.
- **Protect your passwords** and change them regularly.
- Follow procedures for updating contact or payment details.
- **Never give your password** or security information.
- If in doubt - **talk to your IT department**.

## Personal data scam emails

Attackers are sending emails to personal and business email addresses alleging that their data has been sent to the attacker as a result of their account being hacked. The emails include an attachment – a '.dot' file usually titled with the recipient's name. The attacker asks the recipient to view the file to see what information has been hacked. The emails are typical of scam emails in that they are written in poor English.

Users are asked not to click on the links contained in the email.

## NHS.net upgrade scam

Scammers are targeting NHS.net accounts alerting users to an upgrade to improve performance and increase storage.

The email tells users to click on a link and that failure to do so will lead to their account being deactivated.

---

## CASE STUDIES

---

### **Accessing medical records of former girlfriend**

A former administrative employee of an NHS Trust has been prosecuted for accessing the sensitive medical records of her partner's former girlfriend, without the consent of the data controller. The unlawful access to records took place over a 10 month period.

The suspect pleaded guilty to the offence under section 55 of the Data Protection Act and was fined £400, ordered to pay £683.60 prosecution costs and a £40 victim surcharge.

### **Loan shark doctor**

A doctor has been found guilty of running an illegal money lending business from two hospitals, totaling £525,000. The investigation identified that the doctor issued loans ranging from £500 to £50,000 to his customers. The doctor admitted that he knew it was illegal but it would take too long to obtain a license which would have curtailed how much money he was making.

The doctor was given a 10 month prison sentence, suspended for two years, and must pay the money within three months or face a default sentence of five years in prison.

### **Forged timesheets**

A hospital received an anonymous tip off that a ward sister had paid a cheque intended for the hospital's Charitable Fund Department into her private bank account. During the course of the investigation, it was also identified that the ward sister had manipulated her timesheets on 76 occasions to fraudulently claim payment for shifts she had not worked. The fraud amounted to £17,000.

The ward sister pleaded guilty to Fraud by False Representation and Fraud by Abuse of Position.

Sentenced to 12 months' imprisonment.

---

# BRIBERY

---



## What is it?

Bribery is offering an incentive to someone to do something which they wouldn't normally do. For example, someone offering a job might be offered tickets to an event by one of the candidates or someone linked to them.

Think of it as an inducement to secure a favour of some description in return, or giving or receiving something of value to influence a transaction.

Bribery can affect all staff and departments within all NHS organisations, including contractors and suppliers.

In the context of the Bribery Act 2010, the offence of bribery refers to accepting, as well as offering, a bribe.

## Conflicts of interest

Conflicts of interest are closely linked to the offences of bribery. The CCG has a responsibility to safeguard their interests and ensure any conflicts of interest are managed appropriately.

A conflict of interest occurs when a member of staff or an organisation has an interest in another organisation or person, which could possibly corrupt or influence the motivation in an act connected to the organisation.

There are several types of conflicts that could arise:

- direct financial interest;
- indirect financial interest;
- non-financial or personal conflicts; and
- conflict of loyalties.

**If in doubt, declare!**

## A BRIBE OR A GIFT?

Bribery is not restricted to handing over money; the inducement can be an 'advantage'.

Many organisations that do, or seek to do, business with the NHS may seek to influence decision makers, or provide gifts to those in certain roles to create relationships. It is important to consider any gifts or hospitality, or offers of gifts or hospitality, to ensure that the acceptance of it does not give rise to potential conflicts in your role.

Each gift or offer should be considered using the GIFT acronym.

**G**

**Genuine** - is the offer made for reasons of genuine appreciation for something I have done, without any encouragement from me.

**I**

**Independent** - if I accept it, would a reasonable bystander be confident that I could be independent in doing my job.

**F**

**Free** - could I always feel free of any obligation to do something in return for the donor?

**T**

**Transparent** - would I be comfortable if the gift was transparent to my organisation, colleagues and to the public.

NHS England's guide to Managing Conflicts of Interest in the NHS sets out best practice for NHS organisations on dealing with conflicts of interest amongst its staff, as well as providing guidance in relation to gifts, hospitality, secondary employment, and how to best deal with breaches.

---

# WHAT SHOULD I DO IF I SUSPECT FRAUD OR BRIBERY?

## You should

- Report your concerns to the Local Counter Fraud Specialist, Erin Sims.. Alternatively, report your concerns to the Director of Finance or to the NHS Fraud and Corruption Reporting Line on 0800 028 40 60 as soon as possible. Any delay may cause the CCG to suffer further loss.
- Make a note of your concerns.
- Note all relevant details regarding your suspicion ie what was said; significant dates and times; the names of all parties you suspect are involved.
- If possible, retain copies of all relevant supporting documentation ie anything that aroused your suspicions and supports your allegation.

## You should not

- Confront the individual(s) directly.
- Try to investigate the matter yourself.
- Contact the police directly.
- Undertake your own surveillance.
- Convey your own suspicions to anyone else other than those who have the appropriate authority to investigate.
- Do nothing.

If you are unsure about your suspicions or concerns please talk to the LCFS, Erin Sims, as soon as possible. Erin will be able to provide you with appropriate advice and guidance with any issues relating to fraud or bribery. It is important to remember that your concerns maybe important to prevent on-going fraud being committed against the CCG and prevent funds being diverted away from patient care.

---

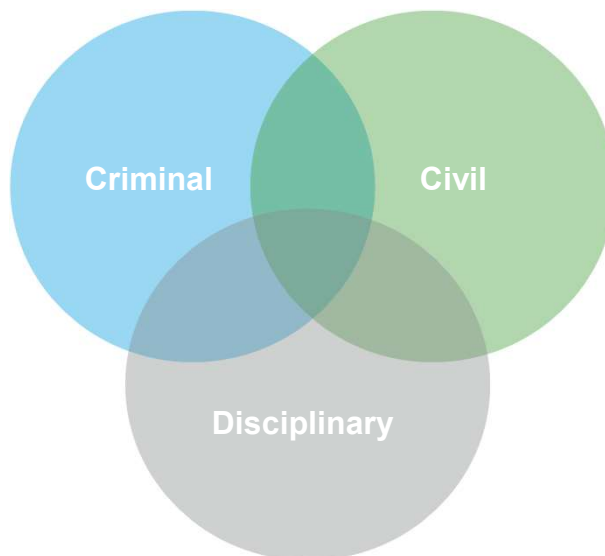
# WHAT COULD HAPPEN TO ME IF I COMMIT FRAUD OR BRIBERY?

---

The CCG has a zero-tolerance approach to fraud. In liaison with the Director of Finance, Human Resources Department, NHS Counter Fraud Authority and the LCFS, the CCG will consider the following sanctions where the allegation has been substantiated. Any one of these, or a combination of them, can be used.

## **Criminal**

A criminal sanction is pursued where evidence of offences has been obtained. A criminal sanction may include imprisonment.



## **Civil**

It may be decided that civil redress is the most appropriate course of action. It is then the responsibility of the organisation to use the civil law to recover any losses; this may include recovery of an employee's NHS pension contributions.

## **Disciplinary**

A separate investigation may be undertaken alongside the criminal investigation but will be run independently. Disciplinary action is a matter for the organisation to decide and may include dismissal.

The matter may also be referred to the relevant professional health body for further investigation. Action may include the subject being struck off the register for their regulatory body.

---

## FOR FURTHER INFORMATION CONTACT

---



**Erin Sims- LCFS  
Manager**

☎: 07800 617456

✉: [erin.sims@nhs.net](mailto:erin.sims@nhs.net)

✉: [erin.sims@rsmuk.com](mailto:erin.sims@rsmuk.com)

### **Director of Finance**

Gareth Kenworthy

**NHS Counter Fraud Authority online  
reporting form at:**

<https://cfa.nhs.uk/reportfraud>

### **Protect**

0207 404 6609



**Kirsty Clarke- LCFS  
Consultant**

☎: 020 3201 8000

✉: [kirsty.clarke8@nhs.net](mailto:kirsty.clarke8@nhs.net)

✉: [kirsty.clarke@rsmuk.com](mailto:kirsty.clarke@rsmuk.com)

### **Freedom to Speak Up Guardian**

Guy Rooney

**National fraud and corruption reporting  
Line**

**(powered by crime stoppers)**

0800 028 40 60

## **RSM UK Tax and Accounting Limited**

25 Farringdon Street  
London  
EC4A 4AB  
T +44 (0)20 3201 8000  
F +44 (0)20 3201 8001  
rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Employer Services Limited, RSM Northern Ireland (UK) Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Before accepting an engagement, contact with the existing accountant will be made to request information on any matters of which, in the existing accountant's opinion, the firm needs to be aware before deciding whether to accept the engagement.