

Buying goods and services

NHS fraud prevention quick guide

v2.0 November 2023

This quick guide highlights the fraud risks when buying goods and services directly from suppliers.

Fraud in this area includes any act whereby deliberate steps are taken to mislead an NHS organisation with a view to dishonestly obtain payments individuals are not entitled to, for example by staff, suppliers or fictitious suppliers or collusion between these groups.

Who is this quick guide for?

This guidance is intended for NHS staff, particularly budget holders, those with responsibility for requisitioning goods and services or approving invoices, and procurement and finance teams, particularly those with responsibility for processing invoices and payments.

How to spot fraud

Staff should remain vigilant to fraud within the process of buying goods and services; here are some areas of vulnerability to be aware of:

- False invoices, where either a legitimate or fabricated supplier dishonestly submits invoices to the NHS for goods or services not supplied.
- Inflated invoices, where a supplier dishonestly submits invoices that do not accurately reflect the goods or services provided or contracted to the NHS.
- Duplicate invoices, where a supplier dishonestly submits more than one invoice for the same goods or service.
- VAT fraud, such as VAT charged on invoices without a VAT registration number and erroneous VAT charges.
- An invoice for goods or services with hidden or incorrect fees, such as: handling fees, add on costs and



administration fees that should not be charged for.

- An invoice from an unfamiliar supplier - this could be someone creating a fictitious supplier and/or shell companies for fraudulent payments.
- Incorrect details listed on the invoice or invoice format which do not match with previous bills received from the supplier. For example, the logo does not match.
- Suppliers with Postal Office boxes or residential addresses.
- Members of staff requesting to specifically deal with particular suppliers.
- No apparent requirement for the goods or services mentioned in the invoice.
- Bank details changed on a supplier's account that has not conducted work for a substantial period of time. (See below for associated NHS fraud prevention quick guide on mandate fraud).

NHSCFA has identified five main (NHS eClass system) categories of spend that have higher levels of non-purchase order spend. These are:

- D: Pharmaceuticals Blood Products & Medical Gases
- M: Hotel Services Equipment Materials & Services
- P: Building & Engineering Products & Services
- X: Transportation
- Z: Staff & Patient Consulting Services & Expenses.

Non-purchase order spend is not fraud, *but* where non-PO spend occurs, an organisation is exposed to a far greater risk of fraud in the procurement process.

How to stop fraud

Millions of invoices are processed each year within the NHS. The NHS buys and pays for these goods and services in a variety of ways. As part of the NHS eProcurement Strategy, the government are encouraging all NHS providers to use purchase to pay (P2P) systems for their non-pay and non-pharmacy expenditure.

NHS organisations should use an electronic P2P accounts payable system with key controls around separation of duties between requisitioning, ordering, checking receipt of goods and services and authorising payment.

Control measures

- You should control your organisation's NHS spend by using a P2P or purchase order

(PO) system (this provides an audit trail and thereby adds an extra layer of scrutiny to purchasing activity and greater assurance in mitigating fraud risk).

- You should monitor and note the rate and value of non-compliant transactions and spend against your established control mechanisms.
- You should record the total amount of spend on goods and services that are PO and non-PO spend.
- Ensure that your organisation's Standing Financial Instructions stipulate that a P2P system is used for all goods and services expenditure.
- Ensure appropriate segregation of duties and job rotation to increase protection from fraud and error. This is achieved by dividing a process between two or more people so that no one person is responsible for the entire purchasing process.
- Only suitable authorised individuals should have access to invoice processing tools within the payment systems.

Preventative action

NHS organisations should require suppliers to provide as much information as possible on invoices, in particular, a full breakdown of the amount due. All invoices should be verified by staff to ensure that:

- The supplier's details including trading name and logos are genuine. If in doubt, check against records and details held on file.
- The supplier's invoicing address and contact details for queries relating to the invoice are checked against records on file.
- The PO number is correct. Staff should be vigilant for any irregularities, for example an extra digit or letter.
- The invoice, account and VAT numbers are consistent, and VAT numbers are valid. UK VAT number can be checked online at <https://www.gov.uk/check-uk-vat-number> and for any EU VAT check online at http://ec.europa.eu/taxation_customs/vies/.
- The NHS organisation's name and invoicing address are correct.
- The supplier's bank details, including account name, number and sort code, are correct. If in doubt, cross check details held on file.
- A full breakdown of the amount being invoiced is provided, including VAT, additional fees and discounts, as applicable.

Process

Other measures to prevent fraud include:

- Staff should spot check information on invoices against supplier details already held on file.
- In conjunction with procurement teams, staff should carry out an exercise of reconciliation of POs, where possible, or booking confirmations and goods received against invoices.
- Staff should approve all invoices in accordance with their NHS organisation's Standing Financial Instructions.
- The organisation should use a payment system which is able to identify duplicate invoices.
- The organisation should establish and run systems and processes that manage conflicts of interest.
- NHS organisations should reinforce existing financial guidance and controls over the processing of payment through the P2P system. Staff should be held to account when procedures are not followed.
- Clear written instructions and procedures should be in place for all staff involved in the payment process, including finance and procurement teams.
- Duties and responsibilities should be made clear to the budget holder/ approver/ requisitioner at the point of accountability.

If you suspect fraud

If fraud is suspected the organisation's escalation process should be followed immediately and the Local Counter Fraud Specialist contacted for advice (see also how to report fraud below).

How to report fraud

Report any suspicions of fraud to the NHS Counter Fraud Authority online at <https://cfa.nhs.uk/reportfraud> or through the NHS Fraud and Corruption Reporting Line **0800 028 4060** (powered by Crimestoppers). All reports are treated in confidence and you have the option to report anonymously.

You can also report fraud to your nominated Local Counter Fraud Specialist.

Why take action?

A significant percentage of the NHS's non-pay spend is used on its operating costs, and in spite of this high value, the NHS Counter Fraud Authority only receives a relatively small number of fraud reports. We therefore judge this area of fraud to be vastly under reported.

By employing policies and procedures such as regular checking that invoiced payments are appropriate, the opportunity for fraud can be minimised, or fraud can be detected at an

early stage. Implementing fraud prevention action within NHS organisations will reduce the associated risks and the potential for significant monetary losses as well as provide assurance to the Audit and Risk Committee that processes, and procedures are being adhered to.

Further information

- The NHSCFA series of fraud prevention quick guides focuses on specific areas of fraud risk vulnerability in NHS finance and procurement and are available to all on [NHSCFA's website](#). They include:
 - » Contract splitting (disaggregate spend)
 - » Contract reviews
 - » Due diligence
 - » Suppliers code of practice: preventing fraud, bribery and corruption
 - » Mandate fraud
 - » Petty cash
 - » Credit card

- NHSCFA has developed and published advice and guidance for the NHS on fraud risks relating to COVID-19, which may be helpful. Please visit [NHSCFA's website](#) for further information.

- The [NHS Fraud Reference Guide](#) was developed by NHSCFA to include information and definitions for different types of NHS fraud.

- For further reading and information on conflicts of interests refer to [NHS England's Conflicts of Interest Guidance](#).

- Details of your Local Counter Fraud Specialist.

Space for business card / contact information