NHS
Counter Fraud Authority

# Buying goods and services

NHS fraud prevention quick guide v3.0 Februrary 2026

## 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.

When buying goods and services, the **Procurement Act 2023** and the **NHS Provider Selection** Regime provides the NHS a simpler, more transparent procurement system by requiring use of a central digital platform and clearer publication of tender and contract information. It also strengthens fraud prevention through greater transparency, mandatory performance reporting, and a central debarment list that blocks suppliers linked to bribery, corruption, or fraud. These changes help the NHS improve accountability, reduce procurement risks, and secure better value for money.

## 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

NHS staff involved in buying goods and services should remain vigilant to a wide range of fraud risks. Procurement fraud affects NHS budgets, disrupts services, and can be facilitated by both external suppliers and internal staff. Remaining alert, following proper processes, and reporting concerns early are key to prevention.

Staff should regularly liaise with their Local Counter Fraud Specialists for information on new and emerging procurement fraud risks; here are some areas of vulnerability to be

aware of:

- Conflicts of interest or collusion between staff and suppliers, influencing procurement decisions unfairly.
- Tender manipulation or bid-rigging, where specifications or processes are shaped to favour certain suppliers.
- Invoice fraud, including false, inflated, duplicate, or unnecessary invoices designed to extract improper payments.
- Hidden or incorrect charges, such as unjustified add-on fees or incorrect VAT applied to invoices.
- High-risk suppliers, including ghost/fake vendors or those presenting suspicious or inconsistent details.
- Mandate fraud or supplier account takeover, where fraudsters alter supplier bank details to divert payments.
- Cyber-enabled fraud, such as phishing emails impersonating suppliers to influence payment instructions.
- Sub-standard or substituted goods, where cheaper or lower-quality items are supplied instead of contracted products.
- Fraudulent contract variations, including unjustified claims for extra work, costs, or extended services.
- Unauthorised recurring charges, where hidden subscription or renewal fees are added without approval.
- Weak supplier due diligence, increasing exposure to unreliable, high-risk, or fraudulent vendors.
- Staff behaviour red flags, like individuals insisting on dealing only with specific suppliers.
- Misuse of purchasing cards or petty cash, where funds are used for personal or non-approved purposes.

## Cyber-Enabled and Artificial Intelligence (AI) enabled Fraud

Many sectors including the NHS are adopting AI technology within existing systems and processes; AI is seen to be beneficial as it can improve efficiency and service delivery. While AI offers significant benefits its widespread adoption by threat actors (fraudsters) also introduces serious challenges that cannot be overlooked. AI tools can be used to target NHS procurement processes, exploit digital platforms, to manipulate payments and supplier details (Cyber-enabled fraud). There is a potential that AI technology will rapidly accelerate the sophistication and volume of fraud threats against NHS systems. For instance, generative AI enables the creation of:

- Deepfake impersonation, including AI-generated voice cloning and synthetic audio/video used to mimic suppliers or staff.

- AI-enhanced fraudulent documents, such as highly convincing fake invoices, websites, and supplier correspondence that replicate logos, formatting, and branding.
- Realistic phishing and social-engineering attempts, including credible emails, messages, and platforms used to trick staff into sharing information or authorising payments.
- Compromised supplier email accounts, where hackers send fraudulent invoices or bank-detail change requests from legitimate addresses.
- Fake procurement platforms or websites created to imitate official portals and fraudulently capture orders or payments.
- Fraudulent QR codes embedded in invoices, redirecting staff to fraudulent payment portals that bypass verification.
- Live impersonation via communication tools, such as fraudsters posing as suppliers or internal colleagues on Teams or email to request urgent actions.
- Data manipulation, where information is altered to support fraudulent payments or conceal suspicious activity.

The following are key eClass categories for high-value spend on goods and services that are highly vulnerable to fraud due to high levels of non-purchase order (non-PO) spend, bribery, or contract manipulation.

- D: Pharmaceuticals, Blood Products & Medical Gases - Extremely high spend volume. Vulnerable to supplier overcharging, diversion of medication, and fraudulent invoicing.
- M: Hotel Services Equipment, Materials & Services - Covers catering, cleaning, and laundry. High risk for "invoice scams" (office supply scams) and fraudulent invoices for services not rendered.
- P: Building & Engineering Products & Services - Vulnerable to tender rigging, contractor collusion, and contract splitting (breaking contracts into smaller, non-tendered amounts).
- X: Transportation - High risk associated with ambulance services, patient transport, and courier contracts, particularly regarding falsified mileage or trip reporting.
- Z: Staff & Patient Consulting Services & Expenses - High risk, particularly regarding the use of non-framework employment agencies to fill shifts at inflated rates ("break glass" options), leading to collusion.

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, NHS providers should adopt the latest approved P2P systems and digital invoice verification tools to strengthen fraud prevention and compliance.

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 your organisation's latest Standing Financial Instructions (SFIs) mandate the use of an approved P2P system for all goods and services expenditure, in line with current NHS procurement policy.
- 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.
- Enforce multi-factor authentication (MFA) for email and finance 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 SFIs.
- Review contracts for hidden clauses; monitor recurring payments and set alerts.
- 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.
- NHS organisation should only use approved NHS procurement platforms; validate URLs and supplier credentials.
- Prohibit the use of QR-based payments and ensure all payments go through official NHS systems.
- Train staff on phishing and AI-driven social engineering; verify urgent voice/video and written requests.
- NHS organisations should consider investment in strengthening cyber security tools.
- Enhanced validation (video ID checks, targeted questioning, layered controls) and data contamination awareness to detect AI-driven fraud.

## 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 (NHSCFA) 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 **Pre-Contract Procurement Fraud and Corruption: Guidance for prevention and detection** 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