NHS
Counter Fraud Authority

Invoice and mandate fraud

Guidance for prevention and detection

October 2022 | Version 2.0

Contents

INVOICE AND MANDATE FRAUD

Introduction

1.1 The NHS Counter Fraud Authority (NHSCFA) is a special health authority charged with identifying and preventing fraud and other economic crime within the NHS and wider health group. The NHSCFA provides the NHS with the support and guidance to enable effective counter fraud responses at national and local level.

1.2 As a health authority focused entirely on counter fraud work, the NHSCFA is independent from other NHS bodies and directly accountable to the Department of Health and Social Care (DHSC).

1.3 We estimate that the NHS is vulnerable to over £1.2 billion worth of fraud each year (as per the NHSCFA Strategic Intelligence Assessment (SIA).[1] We work collaboratively with Local Counter Fraud Specialists (LCFSs) and other stakeholders to understand fraud threats, vulnerabilities, and enablers. We deliver intelligence led counter fraud services to find, respond to and prevent fraud.

1.4 The term 'fraud' refers to a range of economic crimes, such as fraud, bribery and corruption or any other illegal acts committed by an individual or group of individuals to obtain a financial or other gain.

1.5 This document provides LCFSs with guidance which can be used to support work to prevent, detect and investigate the most common kinds of invoice and mandate fraud at a local level. It provides an overview of the invoice environment, provides practical advice on the most effective ways of preventing invoice and mandate fraud and the reporting procedures. It includes advice on raising awareness and is intended to supplement existing policies, directives, and guidance available more widely in the NHS, by providing an overview of NHS invoice and mandate processes from a counter fraud perspective.

1.6 Section 3-6 in this document cover the four main categories of invoice and mandate fraud:

- Insider fraud
- Supplier fraud
- Mandate fraud
- Business Email Compromise fraud.

Each section provides a description of the fraud category and advice on prevention and detection.

1. Strategic Intelligence Assessment | NHS Counter Fraud Authority (cfa.nhs.uk)

Role of the NHSCFA in quality assurance

1.7 In accordance with the Secretary of State Directions to NHS Bodies on Counter Fraud Measures 2017, standard commissioning contracts and the NHS Digital Counter Fraud Manual, all LCFSs should work proactively to deter and prevent fraud in NHS organisations, as well as respond to incidents of fraud

1.8 Under the NHS Standard Contract, all organisations providing NHS services must put in place and maintain appropriate counter fraud arrangements, having regard to NHSCFA requirements. NHS organisations which commission the services should review providers' arrangements to make sure they meet the requirements under the contract

1.9 NHSCFA have launched a suite of standard requirements tailored to enable NHS organisations to meet the Government Functional Standards Gov13. This formally replaces our existing NHS specific standards for fraud, bribery, and corruption. This includes the requirement that the organisation employs or contracts in an accredited person (or persons) nominated to the NHSCFA to undertake the full range of counter fraud, bribery, and corruption work, including proactive work to prevent and deter fraud, bribery and corruption and reactive work to hold those who commit fraud, bribery, and corruption to account

1.10 This document aims to assist LCFSs in identifying potential areas of invoice and mandate fraud risk within their organisations, so that proactive exercise can be undertaken if appropriate

Scale of invoice and mandate fraud

1.11 There is no generally agreed definition of invoice fraud. For the purposes of this guidance document, invoice fraud may be defined as deliberate deception intended to influence any stage of the Purchase-to-Pay (P2P) cycle in order to make a financial gain or cause a loss

1.12 The P2P cycle is the part of the business process which covers requisitioning (purchase ordering), receiving, paying for, and verifying the supply of goods and services and is distinct from the tendering process. Millions of invoices are processed each year within the NHS and the manner in which the NHS procures and pays for goods and services varies

1.13 NHS health bodies purchase goods and services in a number of ways:

- directly from suppliers
- independent distributors
- NHS Supply Chain or
- via collaborative procurement hubs.

1.14 In addition, some health bodies have set up their own collaborative purchasing arrangements, either with neighbouring health bodies or covering particular types of supplies. The P2P processes for ordering supplies and processing invoices in the NHS are not standardised, and although some health bodies have developed improved systems in collaboration with others, this is not general practice. Most health bodies use an electronic accounts payable system, with key controls around separation of duties between requisitioning, ordering, checking receipt of goods and services and authorising payment.

1.15 The NHS uses a number of shared services providers for the provision of invoicing and financial services. It also uses formal outsourced models where an external third party is paid to provide a service that was previously internal to the buying organisation. One formal outsourced solution is NHS Shared Business Services (SBS).

1.16 Recent information suggests that NHS non-pay spend is approximately £27 billion per annum, typically 30% of operating costs. In spite of this high value, the NHSCFA only receives a relatively small number of fraud reports split evenly between the pre and post contract award phase. The NHSCFA assesses that fraud in this area remains vastly under reported. It is considered likely that this is due in part to a high and increasing reliance upon volume-based payments and assurance processes that have historically been unsuccessful in identifying fraud within the NHS.

1.17 The remaining sections of the document will focus on the three main categories of invoice fraud. Each section provides a description of the fraud type, a summary of appropriate prevention measures in relation to key areas, advice on detection and an illustrative case example. The three categories are:

- insider fraud
- supplier fraud
- mandate fraud.

These sections are followed with further information on how LCFSs and their organisations can increase awareness and report the issue.

Insider fraud

2.1 Insider invoice fraud 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. An insider refers to an employee, contractor or individual with legitimate access to the organisations systems. Examples of insider fraud include:

- False payment requests. These occur when an insider creates a false payment instruction with forged signatures, submits it for processing and takes advantage of the lack of time which typically occurs during busy periods to get false invoices approved and paid
- Fraud relating to billing, for instance:
  - an insider overbilling a debtor and pocketing the difference
  - recording false credits, rebates, or refunds
  - creating overpayments to creditors and then pocketing subsequent refunds
  - creating fictitious suppliers and/or shell companies for fraudulent payments
- Fraud relating to procurement (post-contract phase), for instance:
  - an insider altering legitimate purchase orders
  - falsifying documents to obtain authorisation for payment
  - forging signatures on payment authorisations
  - submitting false invoices from fictitious or actual suppliers for payment
  - making improper changes to supplier payment terms or other supplier details
  - intercepting payments to suppliers
  - colluding with a supplier to have marked-up invoices submitted to the health body

Prevention

2.2 The creditor payment system is fundamental to all health bodies. Controls that should be in place to prevent fraud include:

Process

- Ensure appropriate due diligence checks are undertaken on new and existing suppliers
- Reconciliation of purchase orders, booking confirmations, and goods received against invoices
- Supervisors regularly spot-checking supplier records, files, and transactions.
- Maintaining an up-to-date list of authorisers
- Disbursement information is safeguarded from loss or destruction
- Regularly review and remove as appropriate any unused suppliers still active on payee list
- Establishing and running systems and processes for managing conflicts of interest. This is just one aspect of good governance, a failure to acknowledge, identify and address a conflict of interest may result in poor decision, legal challenge, and reputational damage. NHS organisations should follow NHS England's guidance on managing conflicts of interest[2]. This guidance introduces common principles and rules for managing conflicts of interest, provides simple advice to staff and organisations about what to do in common situations. The guidance came into force on 1 June 2017 and is applicable to the following organisations:
- Integrated Care Boards (ICBs) via the statutory guidance issued by NHS England
- NHS Trusts and NHS Foundation Trusts – which includes secondary care trusts, mental health trusts, community trusts, and ambulance trusts, NHS

Payment systems

- Procedures covering the granting and removal of appropriate access rights to users, e.g. based on levels of seniority, appropriate to job roles, controls around time period/duration of access
- Segregation of duties and ensuring appropriate levels of access with respect to accessing invoice processing tools in payment systems
- Staff involved in the procurement cycle to use multi factor authentication (MFA) in respect of email access
- Requirement for users to change their passwords on a regular basis, and separate, strong passwords for each account. Automatic user logout when the system has not been used for a specified amount of time
- System login blocked after a specified number of failed attempts.
- Production of exception reports
- The prevention of suspicious bank accounts being entered onto the system, in the event of an instruction from the NHSCFA

Personnel

- Employment checks on new and existing staff to ensure that health bodies are making an informed decision when recruiting staff. Checks include verifying identity, employment history and criminal records. NHS organisations should follow NHS Employer's guidance on employment checks[3].
- Clear written Standing Operating Procedures for all staff with responsibility for making creditor payments
- Clearly defined budget holders for all accounts.

Detection

2.3 Indicators that could give rise to further investigations include:

- Format of the invoice does not match with previous bills received from the supplier. For example, the logo does not match, the information on the invoice does not correspond with details already held on file by the health body, such as the supplier's VAT number or address
- Invoices that appear to have been altered or are incomplete
- Suppliers with PO 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 hasn't been active for a substantial period of time.

2. https://www.england.nhs.uk/ourwork/coi/
3. https://www.nhsemployers.org/articles/background-information-employment-checks-standards

Case example

The Department of Health (DH) - now the Department of Health and Social Care (DHSC) Accounts Payable section became suspicious of a payment to a contractor who had previously worked in the DH Commercial Directorate but had not invoiced the department for over a year.

DH was in the process of transferring its finance operations to a new system. As part of this process a number of purchase order accounts needed to be migrated across. These accounts still had funds left in them which were due on contracts that had not been completed. The accounts needed to be checked to determine whether they should be closed or remain open.

A senior manager within the former NHS Purchasing and Supply Agency (PASA) (now the Crown Commercial Service) was to oversee this process, with a team reporting to him, and was required to report to the DH Procurement team.

Following reconciliation of budget reports, it was found that a payment of £31,960 had been made to a contractor who had not worked in the commercial directorate for over a year. Further investigation found that the associated invoice contained different bank details to those on the previous invoices from that contractor. It was established that the user profiles used to change the bank details and the recipients of the payments were linked to two members of the PASA team.

Internal enquiries prompted a staff member to contact DH Accounts Payable to give an explanation. He stated that he had run an experiment on the new banking system, using his own bank account details; this was mistakenly done on the live system instead of in a test environment. He was instructed to repay the money and eventually did so.

Further checks were carried out against the same bank account, revealing another payment of £25,000 having been made into the account.

The suspect was arrested, admitted receiving both payments and spending £25,000. He was subsequently sentenced to 12 months' imprisonment and ordered to repay the £25,000.

Supplier fraud

3.1 Supplier invoice fraud includes any act whereby a supplier or purported supplier deliberately takes steps to mislead a health body with a view to obtaining payments that were not due. NHSCFA previously identified a number of substantial risks of overpayments due to:

- duplicate invoicing
- including hidden or incorrect fees, such as 'handling fees', 'on-costs' and 'administration fees'
- over-inflated agency commission above contracted rates
- VAT fraud, such as VAT charged on invoices without a VAT registration number
- invoicing for services that were not supplied.

Prevention

3.2 The NHSCFA previously undertook work looking at employment agencies overcharging the NHS. A key finding of this work was that invoices often failed to provide a full breakdown of the amount due, so it was difficult for health bodies to determine whether the correct amount was being paid Suppliers should be required to provide as much information as possible on their invoices, including:

- supplier's trading name and logo
- supplier's invoicing address and contact details for queries relating to the invoice
- purchase order or booking reference number, as applicable
- invoice, account, and VAT numbers
- health body's name and invoicing address
- supplier's bank details including account name, number, and sort code
- full breakdown of the amount being invoiced including VAT, additional fees, and discounts, as applicable.

3.3 Other measures that should be in place to prevent fraud include the following:

Process

- Spot checking information on invoices against supplier details already held on file by the health body
- Reconciliation of purchase orders or booking confirmations and goods received

- against invoices
- A payment system which is able to identify duplicate invoices
- Checking that VAT numbers are valid. An EU VAT number (including the UK) can be checked on-line at http://ec.europa.eu/taxation_customs/vies/.
- Establishing and running systems and processes for managing conflicts of interest (more information regarding NHS England's guidance on managing conflicts of interest is provided in paragraph 2.2 above).

Personnel

- Clear Standing Operating Procedures for all staff involved in the payment process, including the finance department and spending department as appropriate.

Detection

3.4 NHSCFA recommends that health bodies undertake accounts payable audits to identify duplicate payments, incorrect supplier payments, missed discounts, missed rebates, and tax errors.

Case example

A small construction company won a contract to develop a new hospital wing for an NHS health body. It had been a crucial project for the company, one which brought in much needed revenue at a difficult time. One day, when submitting invoices for payment, one of the smaller charges was accidentally duplicated and, it was paid with no questions asked. The company then went on to make more false claims, starting with exaggerated amounts and incorporating into invoices work that was not completed. It was only when staff at the health body realised that the project was 20% over budget, with the work still incomplete, that a closer examination of the claims was carried out. Had the health body employed procedures such as regular supervision of the contractor's work, including regular checking that the invoiced payments were appropriate and the work had been undertaken, the opportunity for fraud would have been minimised, or the contractor's false claims would have been uncovered at a much earlier stage.

Mandate fraud

4.1 Mandate fraud is variously described as ‘change of bank account scams’, ‘payment diversion fraud’ or ‘supplier account takeover fraud’ It occurs when a fraudster gets an organisation to change a direct debit, standing order or bank transfer mandate, by purporting to be from the genuine supplier in order to benefit from unauthorised payments. Details of suppliers are obtained from a range of sources including corrupt staff, publicly announced contracts, and online logs of supplier contracts.

4.2 If you suspect that you have been the victim of a mandate fraud, immediate action is crucial and may prevent any actual loss of NHS funds. LCFSs and Directors of Finance must act immediately and contact the NHS organisation’s bank and advise them of the suspected mandate fraud. The NHS organisation’s bank should be instructed to immediately contact the bank where the fraudulent transfer of NHS funds has been made and request an immediate freeze on the funds transferred into the suspected fraudsters’ account.

Prevention

4.3 Health bodies should ensure that they have robust authorisation and monitoring procedures in place for the creation and changing of bank details including the following:

- Raise staff awareness of social engineering techniques used by an attacker to commit mandate fraud (see more information below regarding social engineering techniques)
- Staff should always verify requests to change supplier details by using established contact details already held on file.
- Ensure the details held on file are correct and have not been subject to recent change which may be a precursor to a mandate fraud
- If a call from an alleged supplier seems suspicious, take a note of the incoming number and call the organisation using established contact details
- Staff should check the authenticity of an email received from a supplier (e.g., the domain name) by using established supplier contact details already held on file. Email changes can be very subtle and should be checked in detail
- The supplier’s contact details should be taken from existing records held by the health body and not from information supplied in the change request
- Assess how much information is made publicly available and how it could be used against your organisation
- Segregation of duties and ensuring appropriate levels of access with respect to invoice processing tools in payment systems
- Suppliers should periodically be asked to confirm information already held by the health body, such as the previous bank account details, registered address, email address, company registration number, company VAT number or the name of the company secretary
- Suppliers should be sent a bank account amendment form for their finance director or company secretary to sign, confirming the change of bank account details
  A model amendment form is available in **Annex A**. Consider asking the supplier to confirm the amount and date of the last payment made to the supplier.
- Information provided on the amendment form should be checked against the health body’s existing records before any change is made.
- Depending on existing P2P processes, Finance staff may check with Procurement colleagues if they have also been informed of the change
  If they have not, then there is an increased likelihood that the change of contact details is fraudulent
- Clear Standing Operating Procedures for all staff involved in the payment process, including the finance department and spending department as appropriate.
- Establishing and running systems and processes for managing conflicts of interest (more information regarding NHS England’s guidance on managing conflicts of interest is provided in paragraph 2.2 above).

Detection

4.4 Indicators that could give rise to further investigations include.

- Telephone requests received suggesting that there is some urgency in making the change of account details
- Email requests from an address that is not on existing health body records
- Emails may contain poor grammar, a change in language from formal to informal, and pressure of urgency to make the payment
- Written requests without the supplier’s logo on the letter, be aware that logo’s are available online

Business Email Compromise (BEC)

4.5 Business Email Compromise, is also known as CEO fraud, is another form of mandate fraud where fraudsters impersonate an organisation’s senior employee in order to defraud the NHS organisation. In most cases the attackers will focus their efforts on those with access to financial systems or personal information, tricking individuals into performing money transfers or disclosing sensitive data. These attacks often make use of previously compromised accounts and utilise social-engineering tactics and techniques. The emails often do not include the usual attachments or links associated with malicious emails as the attacker is already within the organisation’s email environment.

4.6 The signs of how to spot and preventative advice on how to stop BEC fraud is very similar to those in mandate frauds. The use of Multi Factor Authentication can reduce the risk of this particular type of fraud. It is important that payroll staff are acutely aware of these risks when administering employee payroll banking account information.

Social engineering

4.7 Social engineering refers to the psychological manipulation of people and systems into divulging confidential information and performing actions that they otherwise wouldn't. NHS organisations should be aware of the typical methods that fraudsters use to commit fraud:

- Initial contact made via emails to the NHS organisation's generic finance department mailboxes purporting to be from a contractor. This information may be obtained from the NHS organisation's website where information about significant capital projects and associated construction contractors is published. The emails contain a common template with the contractor's name, logo, and genuine office addresses. The emails request information about the procedure to change bank account details for future payments

- The fraudster subsequently sends an email to the contractor purporting to be from the NHS organisation (using a fake email domain and email signature from the NHS organisation's finance department) to request any outstanding invoices due for payment.

- The fraudster will use information (including banking details) on these invoices to gain the trust of the NHS organisation they are attempting to defraud.

- A convincing email purporting to be from a genuine contracted supplier is sent to the NHS organisation, with a request to change bank account details.

- Email correspondence is designed to appear genuine using similar domain names to those they are purporting to be from. The fraudster socially engineer's information from both the NHS organisation and their contractors to appear genuine to both parties. Any suspect emails should be compared against historic correspondence as part of the verification process.

Case example

The finance director of an NHS health body in England describes a case of mandate fraud that happened at their organisation and what they have learnt from it.

"The shared services provider who deals with our financial services received a correspondence appearing to have come from a construction company who had a contract with us to build a £6 million unit. We believe the criminals obtained their information from material available publicly, such as our publicised invoices over £10,000 and press releases about the new building work. The genuine contractor had done nothing wrong. The criminals had managed to open a bank account using the company name. They instructed our provider to change the bank details to theirs. Our estates department agreed an £897,000 interim payment to the contractor. When this payment was released, that money went straight to the criminals' bank account. On big money schemes, it is usual to send large amounts of money in several payments. The criminals just had to wait for the next payment to hit their account. Luckily for us, the fraud was spotted quickly. The contractor called the shared services provider on the day payment was due to ask where the money was. None of us at the trust knew that the bank details had been changed.

"After receiving the call from the supplier, the shared services provider contacted the NHSCFA. The money had already left the account by the time the recipient 's bank was informed. The bank managed to trace some of the funds into overseas banks and £537,000 of the £897,000 was returned to the trust a few days later. This left the trust with a £360,000 shortfall, money earmarked for patient care."

The finance director continues: "We have since adopted the NHSCFA's guidance and improved our systems. I can't stress enough times how important it is for NHS organisations to take notice of alerts sent by the NHSCFA including guidance on the best way to check and process any 'change of bank details' requests. It is not until it happens that you wish you'd taken notice of that alert. Don't be the next victim. Never just accept a phone call, email or fax asking you to change a supplier 's payment details. Always ensure the old bank account details are provided as well. What's the worst that could happen if you pay the old bank account? A genuine supplier won't mind providing the relevant information in hard copy and will probably be glad that you are being careful."

Raising awareness of mandate fraud

5.1 LCFSs should include invoicing redirection and mandate fraud as part of local fraud awareness initiatives and campaigns. This applies particularly to any events such as induction and training delivered to staff in the finance/accounts payable department.

5.2 Directors of Finance should ensure that staff with responsibility for paying or authorising invoices, or for supervising these processes, are made aware of the risk of invoicing fraud in line with the NHSCFA's guidance and intelligence publications.

5.3 The NHSCFA recommends that suppliers are required to complete a standard amendment form when they notify health bodies of a change in bank account details. An example form is attached in Annex A.

5.4 Resources to support LCFSs in delivering local fraud awareness initiatives are available on the NHSCFA's website at https://cfa.nhs.uk/fraud-prevention/fraud-awareness-toolkit.

5.5 LCFSs should work with communications departments in their health bodies to identify ways to raise awareness of invoicing fraud with health body staff. This could include, for example, putting an article in the staff newsletter, developing local posters and leaflets, and making use of available social media channels (in accordance with each health body's social media policies) to reach all staff, and particularly those responsible for any aspect of the purchase-to-pay cycle.

Media relations

5.6 Proactive engagement with the media remains an excellent and cost-effective way to reach large public and NHS audiences with a deterrent, anti-fraud message. TV and radio stations, newspapers and health trade titles have all shown a keen interest in invoice fraud, given the potential scale of losses. At the local level, this should be led by health body communications teams, giving full support to their LCFS.

5.7 The NHSCFA's Media Relations Office will present the national picture on NHS invoice fraud. For information and advice, you can contact media@nhscfa.gov.uk

Reporting suspected fraud and corruption

6.1 With regard to mandate fraud it is important that the NHSCFA is contacted, and it is imperative that action is taken immediately to prevent the loss of NHS funds. Staff should report all instances of mandate fraud to the NHSCFA's LCFS who will contact the NHSCFAs financial investigators by emailing financialinvestigation@nhscfa.gov.uk. The NHS Wales LCFS will contact NHS CFS Wales Head of Counter Fraud or NHS CFSW financial investigators.

6.2 Allegations of fraud or corruption may be received from a number of sources. It is important that there are effective processes in place for staff to report incidents involving invoice fraud and these processes are documented within a SOP or policy and widely communicated to staff. Staff should be supported and encouraged to report and be assured that the incident will be investigated, and appropriate action taken. All incidents involving fraud should be reported to the health body's LCFS or to the NHSCFA.

6.3 In the case of the NHSCFA, referrals will normally be made either by LCFSs or directly by a health body. However, they may come from a number of other sources, such as the police, other law enforcement agencies, members of the public, NHS employees and whistle-blowers.

6.4 There are two easy ways to report fraud to the NHSCFA: through the NHS Fraud and Corruption Reporting Line 0800 028 4060 (available 24/7) or online at https://cfa.nhs.uk/reportfraud. All reports are treated in confidence and there is the option to report anonymously.

Annex A – Example bank account amendment form

SUPPLIER INFORMATION		
Supplier's name:		
Registered address:		
Town:	City:	Postcode:
Telephone number:	Fax number:	
Email address:		
Remittance address (if different from above):		
Telephone number:	Fax number:	
Email address:		
Name of company secretary:		
Company registration number:		
Company VAT number:	Charity number:	

SUPPLIER INFORMATION										
Current details										
Name of bank:						Account number:				
Account number:						Sort code:				
New details										
Name of bank:						Account number:				
Account number:						Sort code:				

DECLARATION			
I declare that the information I have given on this form is correct and complete.			
Request completed by (print full name):			
Date:			
* Please indicate using X			
Finance Director		Company Secretary	

To enable us to deal with your request please return this form as soon as possible to:
fraudprevention@nhscfa.org.uk